

CRS Report for Congress

Received through the CRS Web

The USA PATRIOT Act: A Legal Analysis

April 15, 2002

Charles Doyle
Senior Specialist
American Law Division

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-cv-0845

The USA PATRIOT Act: A Legal Analysis

Summary

The USA PATRIOT Act passed in the wake of the September 11 terrorist attacks. It flows from a consultation draft circulated by the Department of Justice, to which Congress made substantial modifications and additions. The stated purpose of the Act is to enable law enforcement officials to track down and punish those responsible for the attacks and to protect against any similar attacks.

The Act grants federal officials greater powers to trace and intercept terrorists' communications both for law enforcement and foreign intelligence purposes. It reenforces federal anti-money laundering laws and regulations in an effort to deny terrorists the resources necessary for future attacks. It tightens our immigration laws to close our borders to foreign terrorists and to expel those among us. Finally, it creates a few new federal crimes, such as the one outlawing terrorists' attacks on mass transit; increases the penalties for many others; and institutes several procedural changes, such as a longer statute of limitations for crimes of terrorism.

Critics have suggested that it may go too far. The authority to monitor e-mail traffic, to share grand jury information with intelligence and immigration officers, to confiscate property, and to impose new book-keeping requirements on financial institutions, are among the features troubling to some.

The Act itself responds to some of these reservations. Many of the wiretapping and foreign intelligence amendments sunset on December 31, 2005. The Act creates judicial safeguards for e-mail monitoring and grand jury disclosures; recognizes innocent owner defenses to forfeiture; and entrusts enhanced anti-money laundering powers to those regulatory authorities whose concerns include the well being of our financial institutions.

This report, stripped of its citations and footnotes, is available in an abbreviated form as *The USA PATRIOT Act: A Sketch*, CRS REP.NO. RS21203. In addition, much of the information contained here may also be found under a different arrangement in a report entitled, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, CRS REP.NO. RL31200 (Dec. 10, 2001). A wider array of terrorism-related analysis appears on the CRS terrorism electronic briefing book page.

Contents

Introduction	1
Criminal Investigations: Tracking and Gathering Communications	2
Pen Registers and Trap and Trace Devices	5
Communications Records and Stored E-Mail	6
Electronic Surveillance	8
Criminal Investigators' Access to Foreign Intelligence Information ...	8
Protective Measures	10
Foreign Intelligence Investigations	12
FISA	15
Access to Law Enforcement Information	19
Increasing Institutional Capacity	24
Money Laundering	24
Regulation	24
International Cooperation	34
Crimes	35
Forfeiture	40
Alien Terrorists and Victims	49
Border Protection	49
Detention and Removal	50
Victims	52
Other Crimes, Penalties, & Procedures	54
New crimes	54
New Penalties	57
Other Procedural Adjustments	61
Victims	71
Increasing Institutional Capacity	73
Miscellaneous	74

The USA PATRIOT Act: A Legal Analysis

Introduction

Congress passed the USA PATRIOT Act (the Act) in response to the terrorists' attacks of September 11, 2001.¹ The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. It vests the Secretary of the Treasury with regulatory powers to combat corruption of U.S. financial institutions for foreign money laundering purposes. It seeks to further close our borders to foreign terrorists and to detain and remove those within our borders. It creates new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists. Although it is not without safeguards, critics contend some of its provisions go too far. Although it grants many of the enhancements sought by the Department of Justice, others are concerned that it does not go far enough.

The Act originated as H.R.2975 (the PATRIOT Act) in the House and S.1510 in the Senate (the USA Act).² S.1510 passed the Senate on October 11, 2001, 147 *Cong.Rec.* S10604 (daily ed.). The House Judiciary Committee reported out an amended version of H.R. 2975 on the same day, H.R.Rep.No. 107-236. The House passed H.R. 2975 the following day after substituting the text of H.R. 3108, 147 *Cong.Rec.* H6775-776 (daily ed. Oct. 12, 2001). The House-passed version incorporated most of the money laundering provisions found in an earlier House bill, H.R. 3004, many of which had counterparts in S.1510 as approved by the Senate.³ The House subsequently passed a clean bill, H.R. 3162 (under suspension of the rules), which resolved the differences between H.R. 2975 and S.1510, 147 *Cong.Rec.* H7224 (daily ed. Oct. 24, 2001). The Senate agreed, 147 *Cong.Rec.* S10969 (daily

¹ P.L. 107-56, 115 Stat. 272 (2001); its full title is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)."

² H.R. 2975 was introduced by Representative Sensenbrenner for himself and Representatives Conyers, Hyde, Coble, Goodlatte, Jenkins, Jackson-Lee, Cannon, Meehan, Graham, Bachus, Wexler, Hostettler, Keller, Issa, Hart, Flake, Schiff, Thomas, Goss, Rangel, Berman and Lofgren; S.1510 by Senator Daschle for himself and Senators Lott, Leahy, Hatch, Graham, Shelby and Sarbanes.

³ H.R. 3004 was introduced by Representative Oxley for himself and Representatives LaFalce, Leach, Maloney, Roukema, Bentsen, Hookey, Bereuter, Baker, Bachus, King, Kelly, Gillmore, Cantor, Riley, Latourette, Green (of Wisconsin), and Grucchi; and reported out of the House Financial Services Committee with amendments on October 15, 2001, H.R.Rep.No. 107-250. H.R. 3004, as reported out, included Internet gambling amendments that were not included in H.R. 2975/H.R.3108.

ed. Oct. 24, 2001), and H.R. 3162 was sent to the President who signed it on October 26, 2001.

Criminal Investigations: Tracking and Gathering Communications

A portion of the Act addresses issues suggested originally in a Department of Justice proposal circulated in mid-September.⁴ The first of its suggestions called for amendments to federal surveillance laws, laws which govern the capture and tracking of suspected terrorists' communications within the United States. Federal law features a three tiered system, erected for the dual purpose of protecting the confidentiality of private telephone, face-to-face, and computer communications while enabling authorities to identify and intercept criminal communications.⁵

The tiers reflected the Supreme Court's interpretation of the Fourth Amendment's ban on unreasonable searches and seizures.⁶ The Amendment protects private conversations, *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967). It does not cloak information, even highly personal information, for which there is no individual justifiable expectation of privacy, such as telephone company records of calls made to and from an individual's home, *Smith v. Maryland*, 442 U.S. 735 (1979), or bank records of an individual's financial dealings, *United States v. Miller*, 425 U.S. 435 (1976).

Congress responded to *Berger* and *Katz*, with Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2522 (Title III). Title III, as amended, generally prohibits electronic eavesdropping on telephone conversations, face-to-face conversations, or computer and other forms of electronic communications, 18 U.S.C. 2511.⁷ At the same time, it gives authorities a narrowly defined process for electronic surveillance to be used as a last resort in serious

⁴ The Department's proposal, dated September 20, 2001, came with a brief section by section analysis. Both the proposal (*Draft*) and analysis (*DoJ*) were printed as an appendix in *Administration's Draft Anti-Terrorism Act of 2001, Hearing Before the House Comm. on the Judiciary*, 107th Cong., 1st Sess. 54 (2001).

⁵ For a general discussion of federal law in the area prior to enactment of the Act, see, Stevens & Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, CRS REP.NO. 98-327A (Aug. 8, 2001); Fishman & McKenna, *WIRETAPPING AND EAVESDROPPING* (2d ed. 1995 & 2001 Supp.).

⁶ "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," *U.S. Const.* Amend. IV.

⁷ Although there are technical differences, the interception processes are popularly known as wiretapping, electronic eavesdropping, or electronic surveillance. The terms are used interchangeable here for purposes of convenience, but strictly speaking, wiretapping is limited to the mechanical or electronic interception of telephone conversations, while electronic eavesdropping or electronic surveillance refers to mechanical or electronic interception of communications generally.

criminal cases. When approved by senior Justice Department officials,⁸ law enforcement officers may seek a court order authorizing them to secretly capture conversations concerning any of a statutory list of offenses (predicate offenses), 18 U.S.C. 2516.⁹

⁸ “The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of” one or more predicate offense, 18 U.S.C. 2516.

⁹ The predicate offense list includes (a) felony violations of 42 U.S.C. 2274 through 2277 (enforcement of the Atomic Energy Act of 1954), 42 U.S.C. 2284 (sabotage of nuclear facilities or fuel), or of 18 U.S.C. ch. 37 (espionage), ch. 90 (protection of trade secrets), ch. 105 (sabotage), ch. 115 (treason), ch. 102 (riots), ch. 65 (malicious mischief), ch. 111 (destruction of vessels), or ch. 81 (piracy); (b) a violation of 29 U.S.C. 186 or 501(c) (restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under title 18 of the United States Code; (c) any offense which is punishable under 18 U.S.C. 201 (bribery of public officials and witnesses), 215 (bribery of bank officials), 224 (bribery in sporting contests), 844 (d), (e), (f), (g), (h), or (i) (unlawful use of explosives), 1032 (concealment of assets), 1084 (transmission of wagering information), 751 (escape), 1014 (loans and credit applications generally; renewals and discounts), 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), 1510 (obstruction of criminal investigations), 1511 (obstruction of State or local law enforcement), 1751 (presidential and presidential staff assassination, kidnapping, or assault), 1951 (interference with commerce by threats or violence), 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), 1958 (use of interstate commerce facilities in the commission of murder for hire), 1959 (violent crimes in aid of racketeering activity), 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), 1955 (prohibition of business enterprises of gambling), 1956 (laundering of monetary instruments), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), 659 (theft from interstate shipment), 664 (embezzlement from pension and welfare funds), 1030 (*computer abuse felonies*), 1343 (fraud by wire, radio, or television), 1344 (bank fraud), 2251 and 2252 (sexual exploitation of children), 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), 2321 (trafficking in certain motor vehicles or motor vehicle parts), 1203 (hostage taking), 1029 (fraud and related activity in connection with access devices), 3146 (penalty for failure to appear), 3521(b)(3) (witness relocation and assistance), 32 (destruction of aircraft or aircraft facilities), 38 (aircraft parts fraud), 1963 (violations with respect to racketeer influenced and corrupt organizations), 115 (threatening or retaliating against a Federal official), 1341 (mail fraud), 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, or assault), 831 (prohibited transactions involving nuclear materials), 33 (destruction of motor vehicles or motor vehicle facilities), 175 (biological weapons), 1992 (wrecking trains), a felony violation of 1028 (production of false identification documentation), 1425 (procurement of citizenship or nationalization unlawfully), 1426 (reproduction of naturalization or citizenship papers), 1427 (sale of naturalization or citizenship papers), 1541 (passport issuance without authority), 1542 (false statements in passport applications), 1543 (forgery or false use of passports), 1544 (misuse of passports), or 1546 (fraud and misuse of visas, permits, and other documents); (d) any

Title III court orders come replete with instructions describing the permissible duration and scope of the surveillance as well as the conversations which may be seized and the efforts to be taken to minimize the seizure of innocent conversations, 18 U.S.C. 2518. The court notifies the parties to any conversations seized under the order after the order expires, 18 U.S.C. 2518(8).

Below Title III, the next tier of privacy protection covers some of those matters which the Supreme Court has described as beyond the reach of the Fourth Amendment protection – telephone records, e-mail held in third party storage, and the like, 18 U.S.C. 2701-2709 (Chapter 121). Here, the law permits law enforcement access, ordinarily pursuant to a warrant or court order or under a subpoena in some cases, but in connection with *any* criminal investigation and without the extraordinary levels of approval or constraint that mark a Title III interception, 18 U.S.C. 2703.

Least demanding and perhaps least intrusive of all is the procedure that governs court orders approving the government's use of trap and trace devices and pen registers, a kind of secret "caller id", which identify the source and destination of calls made to and from a particular telephone, 18 U.S.C. 3121-3127 (Chapter 206). The orders are available based on the government's certification, rather than a finding of the court, that the use of the device is likely to produce information relevant to the investigation of a crime, any crime, 18 U.S.C. 3123. The devices record no more than the identity of the participants in a telephone conversation,¹⁰ but neither the orders nor the results they produce need ever be revealed to the participants.

The Act modifies the procedures at each of the three levels. It:

offense involving counterfeiting punishable under 18 U.S.C. 471, 472, or 473; (e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States; (f) any offense including extortionate credit transactions under 18 U.S.C. 892, 893, or 894; (g) a violation of 31 U.S.C. 5322 (dealing with the reporting of currency transactions); (h) any felony violation of 18 U.S.C. 2511 and 2512 (interception and disclosure of certain communications and to certain intercepting devices); (i) any felony violation of 18 U.S.C. ch. 71 (obscenity); (j) 49 U.S.C. 60123(b) (destruction of a natural gas pipeline), 46502 (aircraft piracy); (k) 22 U.S.C. 2778 (Arms Export Control Act); (l) the location of any fugitive from justice from an offense described in this section; (m) a violation of 8 U.S.C. 1324, 1327, or 1328; (n) any felony violation of 18 U.S.C. 922, 924 (firearms); (o) any violation of 26 U.S.C. 5861 (firearms); (p) a felony violation of 18 U.S.C. 1028 (production of false identification documents), 1542 (false statements in passport applications), 1546 (fraud and misuse of visas, permits, and other documents) or a violation of 8 U.S.C. 1324, 1327, or 1328 (smuggling of aliens); (p) 229 (*chemical weapons*), 2332 (*terrorist violence against Americans overseas*), 2332a (*weapons of mass destruction*), 2332b (*multinational terrorism*), 2332d (*financial transactions with countries supporting terrorism*), 2339A (*support of terrorist*), 2332B (*support of terrorist organizations*); (r) any conspiracy to commit any of these, 18 U.S.C. 2516(1)(crimes added by the Act in italics). Other than telephone face to face conversations (*i.e.*, electronic communications), the approval of senior Justice Department officials is not required and an order may be sought in any felony investigation, 18 U.S.C. 2516(3).

¹⁰ Or more precisely, they reveal no more than the identity of the numbers assigned to the telephone lines activated for a particular communication.

- permits pen register and trap and trace orders for electronic communications (*e.g.*, e-mail)
- authorizes nationwide execution of court orders for pen registers, trap and trace devices, and access to stored e-mail or communication records
- treats stored voice mail like stored e-mail (rather than like telephone conversations)
- permits authorities to intercept communications to and from a trespasser within a computer system (with the permission of the system's owner)
- adds terrorist and computer crimes to Title III's predicate offense list
- reenforces protection for those who help execute Title III, ch. 121, and ch. 206 orders
- encourages cooperation between law enforcement and foreign intelligence investigators
- establishes a claim against the U.S. for certain communications privacy violations by government personnel
- terminates the authority found in many of these provisions and several of the foreign intelligence amendments with a sunset provision (Dec. 31, 2005).

Pen Registers and Trap and Trace Devices. In section 216, the Act allows court orders authorizing trap and trace devices and pen registers to be used to capture source and addressee information for computer conversations (*e.g.*, e-mail) as well as telephone conversations, 18 U.S.C. 3121, 3123. In answer to objections that e-mail header information can be more revealing than a telephone number, it creates a detailed report to the court, 18 U.S.C. 3123(a)(3).¹¹

¹¹ "Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public the agency shall ensure that a record will be maintained which will identify – (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of the such device.

"(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof)," section 216(b)(1).

The use of pen registers or trap and trace devices was limited at one time to the judicial district in which the order was issued, 18 U.S.C. 3123 (2000 ed.). Under section 216, a court with jurisdiction over the crime under investigation may issue an order to be executed anywhere in the United States, 18 U.S.C. 3123(b)(1)(C), 3127(2).¹²

Communications Records and Stored E-Mail. With respect to chapter 126, relating among other things to the content of stored e-mail and to communications records held by third parties, the law permits criminal investigators to retrieve the content of electronic communications in storage, like e-mail, with a search warrant, and if the communication has been in remote storage for more than 180 days without notifying the subscriber, 18 U.S.C. 2703(a),(b). A warrant will also suffice to seize records describing telephone and other communications transactions without customer notice, 18 U.S.C. 2703(c). In the absence of the probable cause necessary for a warrant but with a showing of reasonable grounds to believe that the information sought is relevant to a criminal investigation, officers are entitled to a court order mandating access to electronic communications in remote storage for more than 180 days or to communications records, 18 U.S.C. 2703(b),(c). They can obtain a limited amount of record information (subscribers' names and addresses, telephone numbers, billing records and the like) using an administrative, grand jury, or trial court subpoena, 18 U.S.C. 2703(c)(1)(C). There is no subscriber notification in record cases. Elsewhere, the court may delay customer notification in the face of exigent circumstances or if notice is likely to seriously jeopardize the investigation or unduly delay the trial, 18 U.S.C. 2705.

In order to streamline the investigation process, the Act, in section 210, adds credit card and bank account numbers to the information law enforcement officials may subpoena from a communications service provider's customer records, 18 U.S.C. 2703(c)(1)(C).¹³

Another streamlining amendment, section 220, eliminates the jurisdictional restrictions on access to the content of stored e-mail pursuant to a court order.

¹² The Justice Department urged the change in the name of expediency, "At present, the government must apply for new pen trap orders in every jurisdiction where an investigation is being pursued. Hence, law enforcement officers tracking a suspected terrorist in multiple jurisdictions must waste valuable time and resources by obtaining a duplicative order in each jurisdiction," *DoJ* at §101. Here and throughout citations to the United States Code (U.S.C.) without reference to an edition refer to the current Code; references to the 2000 edition of the Code refer to the law prior to amendment by the Act.

¹³ Prior to the amendment, "investigators [could] not use a subpoena to obtain such records as credit card number or other form of payment. In many cases, users register with Internet service providers using false names, making the form of payment critical to determining the user's true identity. . . . this information [could] only be obtained by the slower and more cumbersome process of a court order. In fast-moving investigation[s] such as terrorist bombings – in which Internet communications are a critical method of identifying conspirators and in determining the source of the attacks – the delay necessitated by the use of court orders can often be important. Obtaining billing and other information can identify not only the perpetrator but also give valuable information about the financial accounts of those responsible and their conspirators," *DoJ* at §107.

Previously, only a federal court in the district in which the e-mail was stored could issue the order. Under section 220, federal courts in the district where an offense under investigation occurred may issue orders applicable “without geographic limitation,” 18 U.S.C. 2703.¹⁴

The Act, in section 209, treats voice mail like e-mail, that is, subject to the warrant or court order procedure, rather than to the more demanding coverage of Title III once required, *United States v. Smith*, 155 F.3d 1050, 1055-56 (9th Cir. 1998).

Finally, the Act resolves a conflict between chapter 121 and the federal law governing cable companies. Government entities may have access to cable company customer records only under a court order following an adversary hearing if they can show that the records will evidence that the customer is or has engaged in criminal activity, 47 U.S.C. 511(h). When cable companies began offering telephone and other communications services the question arose whether the more demanding cable rules applied or whether law enforcement agencies were entitled to ex parte court orders under the no-notice procedures applicable to communications providers.¹⁵ The Act makes it clear that the cable rules apply when cable television viewing services are

¹⁴ Speaking of the law before amendment, DoJ explained, “Current law requires the government to use a search warrant to compel a provider to disclose unopened e-mail. 18 U.S.C. §2703(a). Because Federal Rule of Criminal Procedure 41 requires that the ‘property’ to be obtained ‘be within the district’ of the issuing court, however, the rule may not allow the issuance of §2703(a) warrants for e-mail located in other districts. Thus, for example, where an investigator in Boston is seeking electronic e-mail in the Yahoo! account of a suspected terrorist, he may need to coordinate with agents, prosecutors, and judges in the Northern District of California, none of whom have any other involvement in the investigation. This electronic communications information can be critical in establishing relationships, motives, means, and plans of terrorists. Moreover, it is equally relevant to cyber-incidents in which a terrorist motive has not (but may well be) identified. Finally, even cases that require the quickest response (kidnappings, threats, or other dangers to public safety or the economy) may rest on evidence gathered under §2703(a). To further public safety, this section accordingly authorizes courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of their counterparts in other districts where major Internet service providers are located,” *DoJ* at §108.

¹⁵ See e.g., *DoJ* at §109 (“Law enforcement must have the capability to trace, intercept, and obtain records of the communications of terrorists and other criminals with great speed, even if they choose to use a cable provider for their telephone and Internet service. This section amends the Cable Communications Policy Act (‘Cable Act’) to clarify that when a cable company acts as a telephone company or an Internet service provider, it must comply with the same laws governing the interception and disclosure of wire and electronic communications that apply to any other telephone company or Internet service provider. The Cable Act, passed in 1984 to regulate various aspects of the cable television industry, could not take into account the changes in technology that have occurred over the last seventeen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. Because of perceived conflicts between the Cable Act and laws that govern law enforcement’s access to communications and records of communications carried by cable companies, cable providers have refused to comply with lawful court orders, thereby slowing or ending critical investigations”).

involved and that the communications rules of chapter 121 apply when a cable company or anyone else provides communications services, section 211.

Electronic Surveillance. To Title III's predicate offense list, the Act adds cybercrime (18 U.S.C. 1030) and several terrorists crimes, sections 201, 202.¹⁶ A second cybercrime initiative, section 217, permits law enforcement officials to intercept the communications of an intruder within a protected computer system (*i.e.*, a system used by the federal government, a financial institution, or one used in interstate or foreign commerce or communication), without the necessity of a warrant or court order, 18 U.S.C. 2511(2)(i). Yet only the interloper's intruding communications, those to or from the invaded system, are exposed under the section. The Justice Department originally sought the change because the law then did not clearly allow victims of computer trespassing to request law enforcement assistance in monitoring unauthorized attacks as they occur.¹⁷

Criminal Investigators' Access to Foreign Intelligence Information. The Act clearly contemplates closer working relations between criminal investigators and foreign intelligence investigators, particular in cases of international terrorism.¹⁸ It amends the Foreign Intelligence Surveillance Act (FISA) to that end. As originally enacted, the application for a surveillance order under FISA required certification of the fact that "*the purpose for the surveillance is to obtain foreign intelligence information,*" 50 U.S.C. 1804(a)(7)(B)(2000 ed.) (emphasis added), although it anticipated that any evidence divulged as a result might be turned over to law enforcement officials. Defendants often questioned whether authorities had used a FISA surveillance order against them in order to avoid the predicate crime threshold for a Title III order. Out of these challenges arose the notion that perhaps "*the purpose*" might not always mean the sole purpose. The case law indicated that, while an expectation that evidence of a crime might be discovered did not preclude a FISA order, at such time as a criminal prosecution became the focus of the investigation

¹⁶ 18 U.S.C. 229 (chemical weapons), 2332(terrorist acts of violence committed against Americans overseas), 2332a(use of weapons of mass destruction), 2332b(acts of terrorism transcending national boundaries), 2332d(financial transactions with countries which support terrorists), 2339A(providing material support to terrorists), and 2339B(providing material support to terrorist organizations).

¹⁷ "Because service providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves as permitted under current law, they often have no way to exercise their rights to protect themselves from unauthorized attackers. Moreover, such attackers can target critical infrastructures and engage in cyberterrorism," *DoJ* at §106. Elsewhere the Act defines "electronic surveillance" for purposes of the Foreign Intelligence Surveillance Act (FISA) to emphasize that the law enforcement authority for this intruder surveillance does not confer similar authority for purposes of foreign intelligence gathering, section 1003 (50 U.S.C. 1801(f)(2)).

¹⁸ For a general discussion of federal intelligence and law enforcement cooperation, *see*, Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS REP.NO. RL30252 (Dec. 3, 2001).

officials were required to either end surveillance or secure an order under Title III.¹⁹

The Justice Department sought FISA surveillance and physical search authority on the basis of “a” foreign intelligence purpose.²⁰ Section 218 of the Act insists that foreign intelligence gathering be a “significant purpose” for the request for the FISA surveillance or physical search order, 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B), a more

¹⁹ Before FISA, several lower federal courts recognized a foreign intelligence exception to the Fourth Amendment's warrant clause. It is here that the “primary purpose” notion originated. In *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980), decided after FISA on the basis of pre-existing law, the court declared, “as the district court ruled, the executive should be excused from securing a warrant only when the surveillance is conducted ‘primarily’ for foreign intelligence reasons. We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution.” Subsequent case law, however, is not as clear as it might be: *see e.g., United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984) (“FISA permits federal officials to obtain orders authorizing electronic surveillance ‘for the purpose of obtaining foreign intelligence information.’ The requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of Sec. 1802(b) but also from the requirements in Sec. 1804 as to what the application must contain. The application must contain a certification by a designated official of the executive branch that the purpose of the surveillance is to acquire foreign intelligence information, and the certification must set forth the basis for the certifying officials’s belief that the information sought is the type of foreign intelligence information described”); *United States v. Pelton*, 835 F.2d 1067, 1075-76 (4th Cir. 1987) (“We also reject Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily for the purpose of obtaining foreign intelligence information. . . . We agree with the district court that the primary purpose of the surveillance, both initially and throughout was to gather foreign intelligence information. It is clear that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used . . . as evidence in a criminal trial”); *United States v. Sarkissian*, 841 F.2d 959, 907-8 (9th Cir. 1988) (“Defendants rely on the primary purpose test articulated in *United States v. Truong Dinh Hung*. . . . One other court has applied the primary purpose test. Another court has rejected it . . . distinguishing *Truong*. A third court has declined to decide the issue. We also decline to decide the issue”); *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (“Appellants attack the government's surveillance on the ground that it was undertaken not for foreign intelligence purposes, but to gather evidence for a criminal prosecution. FISA applications must contain, among other things, a certification that the purpose of the requested surveillance is the gathering of foreign intelligence information. . . . Although the evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance”).

²⁰ “Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This section will clarify that the certification of a FISA request is supportable where foreign intelligence gathering is ‘a’ purpose of the investigation. This change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts,” *DoJ* at §153.

demanding standard than the “a purpose” threshold proposed by the Justice Department, but a clear departure from the original “the purpose” entry point. FISA once described a singular foreign intelligence focus prerequisite for any FISA surveillance application. Section 504 of the Act further encourages coordination between intelligence and law enforcement officials, and states that such coordination is no impediment to a “significant purpose” certification, 50 U.S.C. 1806(k), 1825(k).²¹

Protective Measures. The Act reenforces two kinds of safeguards, one set designed to prevent abuse and the other to protect those who assist the government. The sunset clause is perhaps the best known of the Act’s safeguards. Under the direction of section 224, many of the law enforcement and foreign intelligence authorities granted by the Act expire as of December 31, 2005.²² The Act also fills some of the gaps in earlier sanctions available for official, abusive invasions of privacy. Prior law made it a federal crime to violate Title III (wiretapping), chapter

²¹ “(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105.” FISA defines “foreign power” and “agent of a foreign power” broadly, *see* note 33, *infra*, quoting, 50 U.S.C. 1801.

²² “(a) Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a)[sharing grand jury information], 203(c)[procedures for sharing grand jury information], 205 [FBI translators], 208 [seizure of stored voice-mail], 210[subpoenas for communications provider customer records], 211[access to cable company communication service records], 213[sneak and peek], 216[pen register and trap and trace device amendments], 221[trade sanctions], and 222[assistance to law enforcement], and the amendments made by those sections) shall cease to have effect on December 31, 2005.

“(b) With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect,” section 224.

The sections which expire are: 201 and 202 (adding certain terrorism crimes to the predicate list for Title III), 293(b)(sharing Title III information with foreign intelligence officers), 204 (clarifying the foreign intelligence exception to the law enforcement pen register and trap and trace device provisions), 206 (roving foreign intelligence surveillance), 207 (duration of foreign intelligence surveillance orders and extensions), 209 (treatment of voice mail as e-mail rather than as telephone conversation), 212 (service provider disclosures in emergency cases), 214 (authority for pen registers and trap and trace devices in foreign intelligence cases), 215 (production of tangible items in foreign intelligence investigations), 217 (intercepting computer trespassers’ communications), 218 (foreign intelligence surveillance when foreign intelligence gathering is “a significant” reason rather than “the” reason for the surveillance), 219 (nationwide terrorism search warrants), 220 (nationwide communication records and stored e-mail search warrants), 223 (civil liability and administrative discipline for violations of Title III, chapter 121, and certain foreign intelligence prohibitions), and 225 (immunity for foreign intelligence surveillance assistance).

121 (e-mail and communications records), or chapter 206 (pen registers and trap and trace devices).²³ Victims of offenses under Title III and chapter 121 (but not chapter 206) were entitled to damages (punitive damages in some cases) and reasonable attorneys' fees,²⁴ but could not recover against the United States.²⁵ Chapter 121 alone insisted upon an investigation into whether disciplinary action ought to be taken when federal officers or employees were found to have intentionally violated its proscriptions, 18 U.S.C. 2707.

The Act augments these sanctions by authorizing a claim against the United States for not less than \$10,000 and costs for violations of Title III, chapter 121, or the Foreign Intelligence Surveillance Act (FISA), by federal officials, and emphasizing the prospect of administrative discipline for offending federal officials, section 223.

Finally, the Act instructs the Department of Justice's Inspector General to designate an official to receive and review complaints of civil liberties violations by DoJ officers and employees, section 1001.

The second category of protective measures applies to service providers and others who help authorities track and gather communications information. For example, section 815 immunizes service providers who in good faith preserve customer records at the government's request until a court order authorizing access can be obtained.²⁶ Another allows providers to disclose customer records to protect the provider's rights and property and to disclose stored customer communications and records in emergency circumstances, section 212. Under pre-existing law providers could disclose the content of stored communications but not customer records. The Justice Department recommended the changes in the interests of greater protection against cybercrimes committed by terrorists and others.²⁷ A third section,

²³ 18 U.S.C. 2511, 2701, and 3121 (2000 ed.), respectively.

²⁴ 18 U.S.C. 2520 and 2707 (2000 ed.).

²⁵ *Spock v. United States*, 464 F.Supp. 510, 514 n.2 (S.D.N.Y. 1978); *Asmar v. IRS*, 680 F.Supp. 248, 250 (E.D.Mich. 1987).

²⁶ Prior law already granted service providers immunity for disclosure of customer records in compliance with a court access order, 18 U.S.C. 2703(f).

²⁷ "Existing law contains no provision that allows providers of electronic communications service to disclose the communications (or records relating to such communications) of their customers or subscribers in emergencies that threaten death or serious bodily injury. This section amends 18 U.S.C. §2702 to authorize such disclosures if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

"Current law also contains an odd disconnect: a provider may disclose the *contents* of the customer's communications in order to protect its rights or property but the current statute does not expressly permit a provider to voluntarily disclose *non-content* records (such as a subscriber's login records). 18 U.S.C. 2702(b)(5). This problem substantially hinders the ability of providers to protect themselves from cyber-terrorists and criminals. Yet the right to disclose the contents of communications necessarily implies the less intrusive ability to disclose non-content records. In order to promote the protection of our nation's critical infrastructures, this section's amendments allow communications providers to voluntarily disclose both content and non-content records to protect their computer systems," *DoJ* at

section 222 promises reasonable compensation for service providers and anyone else who help law enforcement install or apply pen registers or trap and trace devices,²⁸ but makes it clear that nothing in the Act is intended to expand communications providers' obligation to make modifications in their systems in order to accommodate law enforcement needs.²⁹

Foreign Intelligence Investigations

Although both criminal investigations and foreign intelligence investigations are conducted in the United States, criminal investigations seek information about unlawful activity; foreign intelligence investigations seek information about other countries and their citizens. Foreign intelligence is not limited to criminal, hostile, or even governmental activity. Simply being foreign is enough.³⁰

Restrictions on intelligence gathering within the United States mirror American abhorrence of the creation of a secret police, coupled with memories of intelligence gathering practices during the Vietnam conflict which some felt threatened to chill robust public debate. Yet there is no absolute ban on foreign intelligence gathering in the United States. Congress enacted the Foreign Intelligence Surveillance Act (FISA),³¹ something of a Title III for foreign intelligence wiretapping conducted in this country, after the Supreme Court made it clear that the President's authority to see to national security was insufficient to excuse warrantless wiretapping of suspected terrorists who had no identifiable foreign connections, *United States v. United States District Court*, 407 U.S. 297 (1972). FISA later grew to include procedures for physical searches in foreign intelligence cases, 50 U.S.C. 1821-1829, for pen register and trap and trace orders, 50 U.S.C. 1841-1846, and for access to records from businesses engaged in car rentals, motel accommodations, and storage

§110.

²⁸ Chapter 206 had long guaranteed providers and others reasonable compensation, 18 U.S.C. 3124(c), but section 216 of the Act expands the circumstances under which the authorities may request assistance including requests for the help of those not specifically mentioned in the court order. Section 222 makes it clear the expanded obligation to provide assistance is matched by a corresponding right to compensation.

²⁹ Thus in the name of assisting in the execution of Title III, chapter 121, or chapter 206 order, the courts may not cite the Act as the basis for an order compelling a service provider to make system modifications or provide any other technical assistance not already required under 18 U.S.C. 2518(4), 2706, or 3124(c), *see*, H.R.Rep.No. 107-236, at 62-3 (2001) (emphasis added) ("This Act is not intended to affect obligations under Communications Assistance for Law Enforcement Act [which addresses law enforcement-beneficial system modifications and the compensation to be paid for the changes], nor does the act impose any *additional* technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance").

³⁰ *E.g.*, As amended by section 902 of the Act, "'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, *or international terrorist activities*," 50 U.S.C. 401a(2)(language added by the Act in italics).

³¹ 50 U.S.C. 1801 *et seq.*

lockers, 50 U.S.C. 1861-1863 (2000 ed.). Intelligence authorities gained narrow passages through other privacy barriers as well.³²

In many instances, access was limited to information related to the activities of foreign governments or their agents in this country, not simply relating to something foreign here. FISA, for example, is directed at foreign governments, international terrorists, and their agents, spies and saboteurs.³³ There were and still are extra

³² *E.g.*, 18 U.S.C. 2709 (counterintelligence access to telephone toll and transaction records), 12 U.S.C. 3414 (right to financial privacy), 15 U.S.C. 1681u(fair credit reporting).

³³ “As used in this subchapter: (a) ‘Foreign power’ means – (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

“(b) ‘Agent of a foreign power’ means – (1) any person other than a United States person, who – (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who – (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

“(c) ‘International terrorism’ means activities that – (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended – (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

“(d) ‘Sabotage’ means activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States.

“(e) ‘foreign intelligence information’ means – (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an

safeguards if it appears that an intelligence investigation may generate information about Americans ("United States persons," *i.e.*, citizens or permanent resident aliens).³⁴ The procedures tend to operate under judicial supervision and tend to be confidential as a matter of law, prudence, and practice.

The Act eases some of the restrictions on foreign intelligence gathering within the United States, and affords the U.S. intelligence community greater access to information unearthed during a criminal investigation, but it also establishes and expands safeguards against official abuse. More specifically, it:

- permits "roving" surveillance (court orders omitting the identification of the particular instrument, facilities, or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity)
- increases the number of judges on the FISA court from 7 to 11
- allows application for a FISA surveillance or search order when gathering foreign intelligence is *a significant* reason for the application rather than *the* reason
- authorizes pen register and trap & trace device orders for e-mail as well as telephone conversations
- sanctions court ordered access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses
- carries a sunset provision
- establishes a claim against the U.S. for certain communications privacy violations by government personnel
- expands the prohibition against FISA orders based solely on an American's exercise of his or her First Amendment rights.

agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States," 50 U.S.C. 1801.

³⁴ Strictly speaking for FISA purposes, a United States person "means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section," 50 U.S.C. 1801(i).

FISA. FISA is in essence a series of procedures available to secure court orders in certain foreign intelligence cases.³⁵ It operates through the judges of a special court which prior to the Act consisted of seven judges, scattered throughout the country, two of whom were from the Washington, D.C. area. The Act, in section 208, authorizes the appointment of four additional judges and requires that three members of the court reside within twenty miles of the District of Columbia, 50 U.S.C. 1803(a).

Search and Surveillance for Intelligence Purposes. Unless directed at a foreign power, the maximum duration for FISA surveillance orders and extensions was once ninety days and forty-five days for physical search orders and extensions, 50 U.S.C. 1805(e), 1824(d)(2000 ed.). The Act, in section 207, extends the maximum tenure of physical search orders to ninety days and in the case of both surveillance orders and physical search orders extends the maximum life of an order involving an agent of a foreign power to 120 days, with extensions for up to a year, 50 U.S.C. 1805(e), 1824(d). This represents a compromise over the Justice Department's original proposal which would have set the required expiration date for orders at one year instead of 120 days, *Draft* at §151.³⁶

Section 901 of the Act address a concern raised during the 106th Congress relating to the availability of the FISA orders and the effective use of information gleaned from the execution of a FISA order.³⁷ It vests the Director of Central

³⁵ For a general discussion of FISA prior to enactment of the Act, see, Ba zan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance*, CRS REP.NO. RL30465 (Sept. 18, 2001).

³⁶ See also, *DoJ* at §151, "This section reforms a critical aspect of the Foreign Intelligence Surveillance Act (FISA). It will enable the Foreign Intelligence Surveillance Court (FISC), which presides over applications made by the U.S. government under FISA, to authorize the search and surveillance in the U.S. of officers and employees of foreign powers and foreign members of international terrorist groups for up to a year. Currently, the FISC may only authorize such searches and surveillance for up to 45 days and 90 days, respectively. The proposed change would bring the authorization period in line with that allowed for search and surveillance of the foreign establishments for which the foreign officers and employees work. The proposed change would have no effect on electronic surveillance of U.S. citizens or permanent resident aliens."

Section 314 of the Intelligence Authorization Act for Fiscal Year 2002 (Intelligence Authorization Act), P.L. 107-108, 115 Stat. 1394, 1402 (2001), further amended some of the time limits relating to FISA surveillance and physical searches, extending from 24 hours to 72 hours: (a) the time period during which agents might disseminate or use information secured pursuant to a FISA surveillance or search order but otherwise protected from dissemination or use by the order's minimization requirements; and (b) the permissible duration of emergency surveillance or searches after which surveillance or the search must stop or a FISA order application filed (50 U.S.C. 1801(h)(4), 1821(4)(D), 1805(f), 1824(e)).

³⁷ See e.g., S.Rep.No. 106-352, at 3, 6, 7 (2000) ("The Office of Intelligence Policy and Review (OIPR) in the Department of Justice is responsible for advising the Attorney General on matters relating to the national security of the United States. As part of its responsibilities, the OIPR prepares and presents to the Foreign Intelligence Surveillance Court (FISC) all applications for electronic surveillance and physical searches under the Foreign Intelligence Surveillance Act Agencies have informed the Committee that the FISA application

Intelligence with the responsibility to formulate requirements and priorities for the use of FISA to collect foreign intelligence information. He is also charged with the responsibility of assisting the Attorney General in the efficient and effective dissemination of FISA generated information (50 U.S.C. 403-3(c)).

Pen Registers and Trap and Trace Devices for Intelligence Gathering. Section 214 grants the request of the Department of Justice by dropping requirements which limited FISA pen register and trap and trace device orders to facilities used by foreign agents or those engaged in international terrorist or clandestine intelligence activities, 50 U.S.C. 1842(c)(3)(2000 ed.).³⁸ It is enough that the order is sought as part of an investigation to protect against international terrorism or clandestine intelligence activities and is not motivated solely by an American's exercise of his or her First Amendment rights. Elsewhere (section 505), the Act drops a similar limitation for intelligence officials' access to telephone records, 18 U.S.C.

process, as interpreted by the OIPR is administratively burdensome and, at times, extremely slow. Many applications undergo months of scrutiny before submission to the court because the OIPR prescribes standards and restrictions not imposed by the statute. . . . In particular, the OIPR has been criticized for an overly restrictive interpretation of the FISA 'currency' requirement. This is the issue of how recent a subject's activities must be to support a finding of probable cause that the subject is engaged in clandestine intelligence gathering activities. . . . While existing law does not specifically address "past activities," it does not preclude, and legislative history supports, the conclusion that past activities may be part of the totality of circumstances considered by the FISC in making a probable cause determination. . . . By definition, information collected pursuant to a court order issued under the Foreign Intelligence Surveillance Act is foreign intelligence not law enforcement information. Accordingly, the Committee wants to clarify that the FISA 'take' can and must be shared by the Federal Bureau of Investigation with appropriate intelligence agencies. For the intelligence mission of the United States to be successful, there must be a cooperative and concerted effort among intelligence agencies. Any information collected by one agency under foreign intelligence authorities that could assist another agency in executing its lawful mission should be shared fully and promptly. Only then can the United States Government pursue aggressively important national security targets including, for example, counterterrorist and counternarcotics targets"); *see also*, 147 *Cong.Rec.* S799-803 (daily ed. Feb. 24, 2000)(remarks of Sens. Specter, Torricelli and Biden).

³⁸ "When added to FISA two years ago, the pen register/trap and trace section was intended to mirror the criminal pen/trap authority defined in 18 U.S.C. §3123. The FISA authority differs from the criminal authority in that it requires, in addition to a showing of relevance, an additional factual showing that the communications device has been used to contact an 'agent of a foreign power' engaged in international terrorism or clandestine intelligence activities. This has the effect of making the FISA pen/trap authority much more difficult to obtain. In fact, the process of obtaining FISA pen/trap authority is only slightly less burdensome than the process for obtaining full electronic surveillance authority under FISA. This stands in stark contrast to the criminal pen/trap authority, which can be obtained quickly from a local court, on the basis of a certification that the information to be obtained is relevant to an ongoing investigation. The amendment simply eliminates the 'agent of a foreign power' prong from the predication, and thus makes the FISA authority more closely track the criminal authority," *DoJ* at §155.

2709(b), and under the Right to Financial Privacy Act, 12 U.S.C. 3414(a)(5)(A), as well as the Fair Credit Reporting Act, 15 U.S.C. 1681u.³⁹

Section 214 adjusts the language of the FISA pen register-trap and trace authority to permit its use to capture source and destination information relating to electronic communications (*e.g.*, e-mail) as well as telephone communications, 50 U.S.C. 1842(d). The section makes it clear that requests for a FISA pen register-trap and trace order, like requests for other FISA orders, directed against Americans (U.S. persons) may not be based solely on activities protected by the First Amendment, 50 U.S.C. 1842, 1843.

Third Party Cooperation and Tangible Evidence. As in the case of criminal investigations, the Act has several sections designed to encourage third party cooperation and to immunize third parties from civil liability for their assistance. FISA orders may include instructions directing specifically identified third parties to assist in the execution of the order, 50 U.S.C. 1805(c)(2)(B). The Act permits inclusion of a general directive for assistance when the target's activities are designed to prevent more specific identification, section 206, and immunizes in 50 U.S.C. 1805(h), those who provide such assistance, section 225.⁴⁰

³⁹ Except in the case of certain credit information, these are not court procedures, but written requests for third party records which would otherwise be entitled to confidentiality. Section 505, in response to the Justice Department's suggestion, allows FBI field offices to make the requests, *see DoJ* at §157 ("At the present time, National Security Letter (NSL) authority exists in three separate statutes: the Electronic Communications Privacy Act (for telephone and electronic communications records), the Financial Right to Privacy Act (for financial records), and the Fair Credit Reporting Act (for credit records). Like the FISA pen register/trap and trace authority described above, NSL authority requires both a showing of relevance and a showing of links to an 'agent of a foreign power.' In this respect, they are substantially more demanding than the analogous criminal authorities, which require only a certification of relevance. Because the NSLs require documentation of the facts supporting the 'agent of a foreign power' predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section would streamline the process of obtaining NSL authority, and also clarify the FISA Court can issue orders compelling production of consumer reports").

⁴⁰ When it requested the amendment, the Department of Justice explained that the "provision expands the obligations of third parties to furnish assistance to the government under FISA. Under current FISA provisions, the government can seek information and assistance from common carriers, landlords, custodians and other persons specified in court-ordered surveillance. Section 152 would amend FISA to expand existing authority to allow, 'in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person that a common carrier, landlord, custodian or other persons not specified in the Court's order be required to furnish the applicant information and technical assistance necessary to accomplish electronic surveillance in a manner that will protect its secrecy and produce a minimum of interference with the services that such person is providing to the target of electronic surveillance.' This would enhance the FBI's ability to monitor international terrorists and intelligence officers who are

Prior to the Act, FISA allowed federal intelligence officers to seek a court order for access to certain car rental, storage, and hotel accommodation records, 50 U.S.C. 1861 to 1863 (2000 ed.). The Justice Department asked that the authority be replaced with permission to issue administrative subpoenas for any tangible item regardless of the business (if any) of the custodian.⁴¹ The Act amends the provisions, preserving the court order requirement. Yet it allows the procedure to be used in foreign intelligence investigations, conducted to protect against international terrorism or clandestine intelligence activities,⁴² in order to seize any tangible item regardless of who is in possession of the item, and continues in place the immunity for good faith compliance by third party custodians, section 215.

In a related provision, Section 358 amends the –

- purposes section of the Currency and Foreign Transaction Reporting Act (31 U.S.C. 5311);
- suspicious activities reporting requirements section of that Act (31 U.S.C. 5318(g)(4)(B));
- availability of records section of that Act (31 U.S.C. 5319);
- purposes section of the Bank Secrecy Act (12 U.S.C. 1829b(a));
- the Secretary of the Treasury's authority over uninsured banks and other financial institutions under that Act (12 U.S.C. 1953(a));
- access provisions of the Right to Financial Privacy Act (12 U.S.C. 3412(2)(a), 3414(a)(1), 3420(a)(2); and
- access provisions of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1681v;

trained to thwart surveillance by rapidly changing hotel accommodations, cell phones, Internet accounts, etc., just prior to important meetings or communications. Under the current law, the government would have to return to the FISA Court for an order that named the new carrier, landlord, etc., before effecting surveillance. Under the proposed amendment, the FBI could simply present the newly discovered carrier, landlord, custodian or other person with a generic order issued by the Court and could then effect FISA coverage as soon as technically feasible," *DoJ* at 152.

Section 314 of the Intelligence Authorization Act immunizes those who assist in the execution of either a FISA surveillance or physical search order (50 U.S.C. 1805(i)), 115 Stat. 1402.

⁴¹ "The 'business records' section of FISA (50 U.S.C. §§ 1861 and 1862) requires a formal pleading to the Court and the signature of a FISA judge (or magistrate). In practice, this makes the authority unavailable for most investigative contexts. The time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records sought. Since its enactment, the authority has been sought less than five times. This section would delete the old authority and replace it with a general 'administrative subpoena' authority for documents and records. This authority, modeled on the administrative subpoena authority available to drug investigators pursuant to Title 21, allows the Attorney General to compel production of such records upon a finding that the information is relevant," *DoJ* at §156.

⁴² Section 314 of the Intelligence Authorization Act further amended the section to permit orders relating to investigations "to obtain foreign intelligence information not concerning a United States person" in addition to those conducted to protect against terrorism and clandestine activities, 50 U.S.C. 1861(a)(1).

to clarify and authorize access of federal intelligence authorities to the reports and information gathered and protected under those Acts.⁴³

Access to Law Enforcement Information. Shortly after September 11, sources within both Congress and the Administration stressed the need for law enforcement and intelligence agencies to more effectively share information about terrorists and their activities. On September 14, the Senate Select Committee on Intelligence observed that, “effective sharing of information between and among the various components of the government-wide effort to combat terrorists is also essential, and is presently hindered by cultural, bureaucratic, resource, training and, in some cases, legal obstacles,” H.R.Rep.No. 107-63, at 10 (2001). The Justice Department’s consultation draft of September 20 offered three sections which would have greatly expanded the intelligence community’s access to information collected as part of a criminal investigation. First, it suggested that information generated through the execution of a Title III order might be shared in connection with the duties of any executive branch official, *Draft* at §103.⁴⁴

⁴³ H.R.Rep.No. 107-205, at 60-1 (2001) (“This section clarifies the authority of the Secretary of the Treasury to share Bank Secrecy Act information with the intelligence community for intelligence or counterintelligence activities related to domestic or international terrorism. Under current law, the Secretary may share BSA information with the intelligence community for the purpose of investigating and prosecuting terrorism. This section would make clear that the intelligence community may use this information for purposes unrelated to law enforcement.”)

“The provision would also expand a Right to Financial Privacy Act (RFPA) exemption, currently applicable to law enforcement inquiries, to allow an agency or department to share relevant financial records with another agency or department involved in intelligence or counterintelligence activities, investigations, or analyses related to domestic or international terrorism. The section would also exempt from most provisions of the RFPA a government authority engaged in investigations of or analyses related to domestic or international terrorism. This section would also authorize the sharing of financial records obtained through a Federal grand jury subpoena when relevant to intelligence or counterintelligence activities, investigations, or analyses related to domestic or international terrorism. In each case, the transferring governmental entity must certify that there is reason to believe that the financial records are relevant to such an activity, investigation, or analysis.

“Finally, this section facilitates government access to information contained in suspected terrorists’ credit reports when the governmental inquiry relates to an investigation of, or intelligence activity or analysis relating to, domestic or international terrorism. Even though private entities such as lenders and insurers can access an individual’s credit history, the government is strictly limited in its ability under current law to obtain the information. This section would permit those investigating suspected terrorists prompt access to credit histories that may reveal key information about the terrorist’s plan or source of funding--without notifying the target. To obtain the information, the governmental authority must certify to the credit bureau that the information is necessary to conduct a terrorism investigation or analysis. The amendment would also create a safe harbor from liability for credit bureaus acting in good faith that comply with a government agency’s request for information”).

⁴⁴ See also, *DoJ* at §103, “This section facilitates the disclosure of Title III information to other components of the intelligence community in terrorism investigations. At present, 18 U.S.C. §2517(1) generally allows information obtained via wiretap to be disclosed only to the extent that it will assist a criminal investigation. One must obtain a court order to disclose Title III information in non-criminal proceedings. Section 109 [103] would modify the

Second, it recommended a change in Rule 6(e) of the Federal Rules of Criminal Procedure that would allow disclosure of grand jury material to intelligence officials, *Draft* at §354.⁴⁵

Third, it proposed elimination of all constraints on sharing foreign intelligence information uncovered during a law enforcement investigation, mentioning by name the constraints in Rule 6(e) and Title III, *Draft* at §154.⁴⁶

The Act combines versions of all three in section 203. Perhaps because of the nature of the federal grand jury, resolution of the grand jury provision proved especially difficult. The federal grand jury is an exceptional institution. Its purpose is to determine if a crime has been committed, and if so by whom; to indict the guilty; and to refuse to indict the innocent. Its probes may begin without probable cause or any other threshold of suspicion.⁴⁷ It examines witnesses and evidence ordinarily secured in its name and questioned before it by Justice Department prosecutors. Its

wiretap statutes to permit the disclosure of Title III-generated information to a non-law enforcement officer for such purposes as furthering an intelligence investigation. This will harmonize Title III standards with those of the Foreign Intelligence Surveillance Act (FISA), which allows such information-sharing. Allowing disclosure under Title III is particularly appropriate given that the requirements for obtaining a Title III surveillance order in general are more stringent than for a FISA order, and because the attendant privacy concerns in either situation are similar and are adequately protected by existing statutory provisions.”

⁴⁵ *See also, DoJ* at §354, “This section makes changes in Rule 6(e) of the Federal Rules of Criminal Procedure, relating to grand jury secrecy, to facilitate the sharing of information with federal law enforcement, intelligence, protective, national defense, and immigration personnel in terrorism and national security cases. The section is in part complimentary to section 154 of the bill, relating to sharing of foreign intelligence information, and reflects a similar purpose of promoting a coordinated governmental response to terrorist and national security threats.” Contrary to the implication here section 154 deals with sharing information gathered by law enforcement officials not with information gathered by intelligence officers

⁴⁶ *See also, DoJ* at §154, “This section provides that foreign intelligence information obtained in criminal investigations, including grand jury and electronic surveillance information, may be shared with other federal government personnel having responsibilities relating to the defense of the nation and its interests. With limited exceptions, it is presently impossible for criminal investigators to share information obtained through a grand jury (including through the use of grand jury subpoenas) and information obtained from electronic surveillance authorized under Title III with the intelligence community. This limitation will be very significant in some criminal investigations. For example, grand jury subpoenas often are used to obtain telephone, computer, financial and other business records in organized crime investigations. Thus, these relatively basic investigative materials are inaccessible for examination by intelligence community analysts working on related transnational organized crime groups. A similar problem occurs in computer intrusion investigations: grand jury subpoenas and Title III intercepts are used to collect transactional data and to monitor the unknown intruders. The intelligence community will have an equal interest in such information, because the intruder may be acting on behalf of a foreign power.”

⁴⁷ *Blair v. United States*, 250 U.S. 273, 281 (1919) (the grand jury “is a grand inquest, a body with powers of investigation and inquisition, the scope of whose inquiries is not to be limited narrowly by questions of propriety or forecasts of whether any particular individual will be found properly subject to an accusation of crime”).

affairs are conducted in private and outside the presence of the court. Only the attorney for the government, witnesses under examination, and a court reporter may attend its proceedings, F.R.Crim.P. 6(d). Matters occurring before the grand jury are secret and may be disclosed by the attending attorney for the government and those assisting the grand jury only in the performance of their duties; in presentation to a successor grand jury; or under court order for judicial proceedings, for inquiry into misconduct before the grand jury, or for state criminal proceedings, F.R.Crim.P. 6(e).

The Act, in section 203(a), allows disclosure of matters occurring before the grand jury to “any federal law enforcement, intelligence, protective, immigration, national defense, or national security” officer to assist in the performance of his official duties, F.R.Crim.P. 6(e)(3)(C)(i)(V).⁴⁸

Critics may protest that the change could lead to the use of the grand jury for intelligence gathering purposes, or less euphemistically, to spy on Americans.⁴⁹ The proposal was never among those scheduled to sunset, but earlier versions of the section followed the path used for most other disclosures of grand jury material: prior

⁴⁸ These officers may receive: (1) “foreign intelligence information” that is, information regardless whether it involves Americans or foreign nationals that “[a] relates to the ability of the United States to protect against – (aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; (cc) clandestine intelligence activities by an intelligence service or network of a foreign power;” or [b] “with respect to a foreign power or foreign territory that relates to – (aa) the national defense or security of the United States; or (bb) the conduct of the foreign affairs of the United States,” F.R.Crim.P. 6(e)(3)(C)(iv); (2) when the matters involve foreign intelligence or counterintelligence, that is, [a] “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities” or [b] “information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or *international terrorist activities*,” 50 U.S.C. 401a(2),(3)(language added by section 902 of the Act in italics).

⁴⁹ Beale & Felman, *The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the USA PATRIOT Act's Changes to Grand Jury Secrecy*, 25 HARVARD JOURNAL OF LAW & PUBLIC POLICY 699, 719-20 (2002)(“There is a significant danger that the rule permitting disclosure will be treated as the de facto authorization of an expansion of the grand jury’s investigative role to encompass seeking material relevant only to matters of national security, national defense, immigration, and so forth. The grand jury’s awesome powers should not be unwittingly extended to a much wider range of issues. . . . Since the grand jury operates in secret, there are no public checks on the scope of its investigations, and witnesses are not permitted to challenge its jurisdiction. Only the supervising court is in a position to keep the grand jury’s investigation within proper bounds. Requiring judicial approval of foreign intelligence and counterintelligence information disclosures would provide a natural check against the temptation to manipulate the grand jury to develop information for unauthorized purposes”); *but see*, Scheidegger et al., *Federalist Society White Paper on The USA PATRIOT Act of 2001: Criminal Procedure Sections 6* (Nov. 2001)(“The grand jury secrecy rule is a rule of policy which has always had exceptions, and it has been frequently modified. The secrecy rule has no credible claim to constitutional stature”).

court approval, H.R.Rep.No. 107- 236, at 73 (2001). The Act, in section 203(a), instead calls for confidential notification of the court that a disclosure has occurred and the entity to whom it was made, F.R.Crim.P. 6(e)(3)(C)(iii). It also insists that the Attorney General establish implementing procedures for instances when the disclosure “identifies” Americans (U.S. persons), section 203(c).

Law enforcement officials may share Title III information with the intelligence community under the same conditions, section 203(b),⁵⁰ although the grand jury and Title III sharing provisions differ in at least three important respects. The court need not be notified of Title III disclosures. On the other hand, the authority for sharing Title III information expires on December 31, 2005, section 224, and agencies and their personnel guilty of intentional improper disclosures may be subject to a claim for damages and disciplinary action, 18 U.S.C. 2520.

The third subsection of section 203 remains something of an enigma. It speaks in much the same language as its counterparts. It allows law enforcement officials to share information with the intelligence community, “notwithstanding any other provisions of law,” section 203(d).⁵¹ It either swallows the other subsections, or supplements them. Several factors argue for its classification as a supplement. Congress is unlikely to have crafted subsections (a), (b) and (c) only to completely

⁵⁰ Information derived from a Title III interception may be shared with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security officer if it regards: (1) “foreign intelligence information” that is, information irrespective of whether it involves Americans or foreign nationals that “[A] relates to the ability of the United States to protect against – (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; (iii) clandestine intelligence activities by an intelligence service or network of a foreign power;” or [B] “with respect to a foreign power or foreign territory that relates to – (i) the national defense or security of the United States; or (ii) the conduct of the foreign affairs of the United States;” (2) when the matters involve foreign intelligence or counterintelligence as defined by 50 U.S.C. 401a (as amended by section 902 of the Act), *i.e.*, “As used in this Act: (1) The term ‘intelligence’ includes foreign intelligence and counterintelligence. (2) The term ‘foreign intelligence’ means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, *or international terrorist activities*. (3) The term ‘counterintelligence’ means information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities” (language added by section 902 in italics).

⁵¹ “Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C.) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information,” §203(d)(1). The subsection goes to define “foreign intelligence information” in the same terms used to define that phrase in Title III (18 U.S.C. 2510(19)) and in Rule 6(e)(F.R.Crim.P.6(e)(3)(C)(iv)), §203(d)(2).

nullify them in subsection (d). Without a clear indication to the contrary, the courts are unlikely to find that Congress intended nullification.⁵² By gathering the three into a single section Congress avoided the suggestion that the phrase “notwithstanding any other provision of law” constitutes surplusage. The Title III and grand jury sharing procedures are not in other provisions of law, they are now subsections of the same provision of law. Moreover, Congress seemed to signal an intent for the subsections to operate in tandem when it dropped the language of the original Justice Department proposal which expressly identified Title III and Rule 6(e) as examples of the restrictions to be overcome by the universal sharing language.⁵³

Section 203 deals with earlier legal impediments to sharing foreign intelligence information unearthed during the course of a criminal investigation. Section 905 looks to dissolve the barriers may be more cultural than legal. Under it, the Attorney General is to issue guidelines governing the transmittal to the Director of Central Intelligence of foreign intelligence information that surfaces in the course of a criminal investigation. The section also instructs the Attorney General to promulgate guidelines covering reports to the Director of Central Intelligence on whether a criminal investigation has been initiated or declined based on an intelligence community referral, 50 U.S.C. 403-5b. To ensure effective use of increased information sharing, section 908 calls for training of federal, state and local officials to enable them to recognize foreign intelligence information which they encounter in their work and how to use it in the performance of their duties, 28 U.S.C. 509 note.

Increasing Institutional Capacity. As noted elsewhere, the Act liberalizes authority for the FBI to hire translators, section 203, which enhances its capacity to conduct both criminal and foreign intelligence investigations. The Act also reflects sentiments expressed earlier concerning coordinated efforts to develop a

⁵² *Duncan v. Walker*, 121 S.Ct. 2120, 2125 (2001)(internal quotation marks and parallel citations omitted)(“It is our duty to give effect, if possible, to every clause and word of a statute. *United States v. Menasche*, 348 U.S. 528, 538-539 (1955) (quoting *Montclair v. Ramsdell*, 107 U.S. 147, 152 (1883)); see also *Williams v. Taylor*, 529 U.S. 362, 404 (2000) (describing this rule as a cardinal principle of statutory construction); *Market Co. v. Hoffman*, 101 U.S. 112, 115 (1879)(As early as in Bacon's Abridgment, sect. 2, it was said that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant). We are thus reluctant to treat statutory terms as surplusage in any setting. *Babbitt v. Sweet Home Chapter, Communities for Great Ore.*, 515 U.S. 687, 698 (1995); see also *Ratzlaf v. United States*, 510 U.S. 135, 140 (1994)”).

It is not possible to conclude that Congress intended the universal subsection (d) to apply until sunset and the grand jury and Title III subsections (a), (b), and (c) to operate thereafter, because the Title III subsection expires at the same time as the universal subsection.

⁵³ *Draft at* §154, “Notwithstanding any other provision of law, it shall be lawful for foreign intelligence information obtained as part of a criminal investigation (including, without limitation, information subject to Rule 6(e) of the Federal Rules of Criminal Procedure and information obtained pursuant to chapter 119 of title 18, United States Code [*i.e.* Title III]) to be provided to any federal law enforcement, intelligence, protective, or national defense personnel, or any federal personnel responsible for administering the immigration laws of the United States, or to the President and the Vice President of the United States.”

computerized translation capability to be used in foreign intelligence gathering.⁵⁴ Section 907 instructs the Director of the Central Intelligence, in consultation with the Director of the FBI, to report on the creation of a National Virtual Translation Center. The report is to include information concerning staffing, allocation of resources, compatibility with comparable systems to be used for law enforcement purposes, and features which permit its efficient and secure use by all of the intelligence agencies.

Money Laundering

In federal law, money laundering is the flow of cash or other valuables derived from, or intended to facilitate, the commission of a criminal offense. It is the movement of the fruits and instruments of crime. Federal authorities attack money laundering through regulations, international cooperation, criminal sanctions, and forfeiture.⁵⁵ The Act bolsters federal efforts in each area.

Regulation. Prior to passage of the Act, the Treasury Department already enjoyed considerable authority to impose reporting and record-keeping standards on financial institutions generally and with respect to anti-money laundering matters in particular.⁵⁶

⁵⁴ “The Committee is concerned that intelligence in general, and intelligence related to terrorism in particular, is increasingly reliant on the ability of the Intelligence Community to quickly, accurately and efficiently translate information in a large number of languages. Many of the languages for which translation capabilities are limited within the United States Government are the languages that are of critical importance in our counterterrorism efforts. The Committee believes that this problem can be alleviated by applying cutting-edge, internet-like technology to create a ‘National Virtual Translation Center.’ Such a center would link secure locations maintained by the Intelligence Community throughout the country and would apply digital technology to network, store, retrieve, and catalogue the audio and textual information. Foreign intelligence could be collected technically in one location, translated in a second location, and provided to an Intelligence Community analyst in a third location.

“The Committee notes that the CIA, FBI NSA and other intelligence agencies have applied new technology to this problem. The Committee believes that these efforts should be coordinated so that the solution can be applied on a Community-wide basis. Accordingly, the Committee directs the Director of Central Intelligence, in consultation with the Director of the FBI, and other heads of departments and agencies within the Intelligence Community, to prepare and submit to the intelligence committees by June 1, 2002, a report concerning the feasibility and structure of a National Virtual Translation Center, including recommendations regarding the establishment of such a center and the funding necessary to do so,” S.Rep.No. 107-63, at 11 (2001).

⁵⁵ For a brief overview, see, Murphy, *Money Laundering: Current Law and Proposals*, CRS REP.NO. RS21032 (DEC. 21, 2001).

⁵⁶ See e.g., 12 U.S.C. 1829b (retention or records by insured depository institutions), 1951-1959 (record-keeping by financial institutions); 31 U.S.C. 5311 (“It is the purpose of this subchapter [31 U.S.C. 5311 et seq.] (except section 5315 [relating to foreign current transaction reports]) to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings”).

Records and Reports. For instance, under the Currency and Financial Transaction Reporting Act, a component of the Bank Secrecy Act, anyone who transports more than \$10,000 into or out of the United States must report that fact to the Treasury Department, 31 U.S.C. 5316. Banks, credit unions, and certain other financial institutions must likewise report identifying information relating to cash transactions in excess of \$10,000 to the Treasury Department (CTRs), 31 U.S.C. 5313, 31 C.F.R. §103.22. Other businesses are required to report to the Internal Revenue Service the particulars relating to any transaction involving more than \$10,000 in cash, 26 U.S.C. 6050I. Banks must file suspicious activity reports (SARs) with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) for any transactions involving more than \$5,000 which they suspect may be derived from illegal activity, 31 U.S.C. 5318(g), 31 C.F.R. §103.18. Money transmission businesses and those that deal in traveler's checks or money orders are under a similar obligation for suspicious activities involving more than \$2,000, 31 U.S.C. 5318(g), 31 C.F.R. §103.18.

Among other things, the Act expands the authority of the Secretary of the Treasury over these reporting requirements. He is to promulgate regulations, pursuant to sections 356 and 321, under which securities brokers and dealers as well as commodity merchants, advisors and pool operators must file suspicious activity reports, 31 U.S.C. 5318 note; 31 U.S.C. 5312(2)(c)(1). Businesses which were only to report cash transactions involving more than \$10,000 to the IRS are now required to file SARs as well,⁵⁷ reflecting Congress' view that the information provided the IRS may be valuable for other law enforcement purposes.⁵⁸ This concern is likewise

⁵⁷ Section 365, 31 U.S.C. 5331; Sec. 321, 31 U.S.C. 5312.

⁵⁸ H.R.Rep.No. 107-250, at 38-9 (2001) ("Most importantly, the Committee found significant shortcomings in the use of information already in possession of the government. Section 6050I of the Internal Revenue Code requires that any person engaged in a trade or business (other than financial institutions required to report under the Bank Secrecy Act) file a report with the Federal government on cash transactions in excess of \$10,000. Reports filed pursuant to this requirement provide law enforcement authorities with a paper trail that can, among other things, lead to the detection and prosecution of money laundering activity.

"Under current law, non-financial institutions are required to report cash transactions exceeding \$10,000 to the Internal Revenue Service (IRS) on IRS Form 8300. Because the requirement that such reports be filed is contained in the Internal Revenue Code, Form 8300 information is considered tax return information, and is subject to the procedural and record-keeping requirements of section 6103 of the Internal Revenue Code. For example, section 6103(p)(4)(E) requires agencies seeking Form 8300 information to file a report with the Secretary of the Treasury that describes the procedures established and utilized by the agency for ensuring the confidentiality of the information. IRS requires that agencies requesting Form 8300 information file a 'Safeguard Procedures Report' which must be approved by the IRS before any such information can be released. For that reason, Federal, State and local law enforcement agencies are not given access to the Form 8300s as Congress anticipated when it last amended this statute. See 26 U.S.C. 6103(l)(15).

"While the IRS uses Form 8300 to identify individuals who may be engaged in tax evasion, Form 8300 information can also be instrumental in helping law enforcement authorities trace cash payments by drug traffickers and other criminals for luxury cars, jewelry, and other expensive merchandise. Because of the restrictions on their dissemination outlined above, however, Form 8300s are not nearly as accessible to law enforcement

reflected in section 357 which asks the Secretary of the Treasury to report on the Internal Revenue Service's role in the administration of the Currency and Foreign Transaction Reporting Act (31 U.S.C. 5311 et seq.), and what transfers of authority, if any, are appropriate.

Sections 351 and 355 address the liability for disclosure of suspicious activity reports (SARs). Prior to the Act, federal law prohibited financial institutions and their officers and employees from tipping off any of the participants in a suspicious transaction, 31 U.S.C. 5318(g)(2)(2000 ed.). Federal law, however, immunized the institutions and their officers and employees from liability for filing the reports and for failing to disclose that they had done so, 31 U.S.C. 5318(g)(3)(2000 ed.). Section 351 makes changes in both the immunity and the proscription. It adds government officials who have access to the reports to the anti-tip ban, 31 U.S.C. 5318(g)(2)(A). It allows, but does not require, institutions to reveal SAR information in the context of employment references to other financial institutions, 31 U.S.C. 5318(g)(2)(B). Finally, it makes clear that the immunity does not extend to immunity from governmental action.⁵⁹ Section 355 expands the immunity to cover disclosures in

authorities as the various reports mandated by the Bank Secrecy Act, which can typically be retrieved electronically from a database maintained by the Treasury Department. The differential access to the two kinds of reports is made anomalous by the fact that Form 8300 elicits much the same information that is required to be disclosed by the Bank Secrecy Act. For example, just as Form 8300 seeks the name, address, and social security number of a customer who engages in a cash transaction exceeding \$10,000 with a trade or business, Currency Transaction Reports (CTRs) mandated by the Bank Secrecy Act require the same information to be reported on a cash transaction exceeding \$10,000 between a financial institution and its customer").

⁵⁹ "Subsection (a) of section [351] makes certain technical and clarifying amendments to 31 U.S.C. 5318(g)(3), the Bank Secrecy Act's 'safe harbor' provision that protects financial institutions that disclose possible violations of law or regulation from civil liability for reporting their suspicions and for not alerting those identified in the reports. The safe harbor is directed at Suspicious Activity Reports and similar reports to the government and regulatory authorities under the Bank Secrecy Act.

"First, section [351](a) amends section 5318(g)(3) to make clear that the safe harbor from civil liability applies in arbitration, as well as judicial, proceedings. Second, it amends section 5318(g)(3) to clarify the safe harbor's coverage of voluntary disclosures (that is, those not covered by the SAR regulatory reporting requirement). The language in section 5318(g)(3)(A) providing that 'any financial institution that *** makes a disclosure pursuant to *** any other authority *** shall not be liable to any person' is not intended to avoid the application of the reporting and disclosure provisions of the Federal securities laws to any person, or to insulate any issuers from private rights of actions for disclosures made under the Federal securities laws.

"Subsection [351](b) amends section 5318(g)(2) of title 31--which currently prohibits notification of any person involved in a transaction reported in a SAR that a SAR has been filed--to clarify (1) that any government officer or employee who learns that a SAR has been filed may not disclose that fact to any person identified in the SAR, except as necessary to fulfill the officer or employee's official duties, and (2) that disclosure by a financial institution of potential wrongdoing in a written employment reference provided in response to a request from another financial institution pursuant to section 18(v) of the Federal Deposit Insurance Act, or in a written termination notice or employment reference provided in accordance with the rules of a securities self-regulatory organization, is not prohibited simply because the

employment references to other insured depository financial institutions provided disclosure is not done with malicious intent.⁶⁰

The Financial Crimes Enforcement Network (FinCEN), a component within the Treasury Department long responsible for these anti-money laundering reporting and record-keeping requirements, 31 C.F.R. pt. 103, was administratively created in 1990 to provide other government agencies with an “intelligence and analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes,” 55 *Fed.Reg.* 18433 (May 2, 1990).

The Act, in section 361, makes FinCEN a creature of statute, a bureau within the Treasury Department, 31 U.S.C. 310. Section 362 charges it with the responsibility of establishing a highly secure network to allow financial institutions to file required reports electronically and to permit FinCEN to provide those institutions with alerts and other information concerning money laundering protective measures, 31 U.S.C. 310 note.

Special Measures. In extraordinary circumstances involving international financial matters, the Act grants the Secretary of the Treasury, in consultation with other appropriate regulatory authorities, the power to issue regulations and orders involving additional required “special measures” and additional “due diligence” requirements to combat money laundering. The special measure authority, available under section 311, comes to life with the determination that particular institutions, jurisdictions, types of accounts, or types of transactions pose a primary money

potential wrongdoing was also reported in a SAR,” H.R.Rep.No. 107-250, at 66 (2001).

⁶⁰ 31 U.S.C. 1828(w). “This section deals with the same employment reference issue addressed in section [351] but with respect to title 12. Occasionally banks develop suspicions that a bank officer or employee has engaged in potentially unlawful activity. These suspicions typically result in the bank filing a SAR. Under present law, however, the ability of banks to share these suspicions in written employment references with other banks when such an officer or employee seeks new employment is unclear. Section 208 would amend 12 U.S.C. 1828 to permit a bank, upon request by another bank, to share information in a written employment reference concerning the possible involvement of a current or former officer or employee in potentially unlawful activity without fear of civil liability for sharing the information, but only to the extent that the disclosure does not contain information which the bank knows to be false, and the bank has not acted with malice or with reckless disregard for the truth in making the disclosure,” H.R.Rep.No. 107-250, at 67 (2001).

laundering concern.⁶¹ These special measures may require U.S. financial institutions to:

- maintain more extensive records and submit additional reports relating to participants in foreign financial transactions with which they are involved
- secure beneficial ownership information with respect to accounts maintained for foreign customers
- adhere to “know-your-customer” requirements concerning foreign customers who use “payable-through accounts” held by the U.S. entity for foreign financial institutions
- keep identification records on foreign financial institutions’ customers whose transactions are routed through the foreign financial institution’s correspondent accounts with the U.S. financial institution
- honor limitations on correspondent or payable-through accounts maintained for foreign financial institutions.⁶²

⁶¹ 31 U.S.C. 5318A. The circumstances considered in the case of a suspect jurisdiction are: evidence of organized crime or terrorist transactions there; the extent to which the jurisdiction’s bank secrecy or other regulatory practices encourage foreign use; the extent and effectiveness of the jurisdiction’s banking regulation; the volume of financial transactions in relation to the size of the jurisdiction’s economy; whether international watch dog groups (such as the Financial Action Task Force) have identified the jurisdiction as an offshore banking or secrecy haven; the existence or absence of a mutual legal assistance treaty between the U.S. and the jurisdiction; and the extent of official corruption within the jurisdiction. The institutional circumstances weighed before imposing special measures with respect to particular institutions or types of accounts or transactions include the intent to which the suspect institution or types of accounts or transactions are particularly attractive to money launderers, the extent to which they can be used by legitimate businesses, and the extent to which focused measures are likely to be successful.

⁶² The House report describes these measures in greater detail: “Section [311] adds a new section 5318A to the Bank Secrecy Act, authorizing the Secretary of the Treasury to require domestic financial institutions and agencies to take one or more of five ‘special measures’ if the Secretary finds that reasonable grounds exist to conclude that a foreign jurisdiction, a financial institution operating outside the United States, a class of international transactions, or one or more types of accounts is a ‘primary money laundering concern.’ Prior to invoking any of the special measures contained in section 5318A(b), the Secretary is required to consult with the Chairman of the Board of Governors of the Federal Reserve System, any other appropriate Federal banking agency, the Securities and Exchange Commission, the National Credit Union Administration Board, and, in the sole discretion of the Secretary, such other agencies and interested parties as the Secretary may find to be appropriate. Among other things, this consultation is designed to ensure that the Secretary possesses information on the effect that any particular special measure may have on the domestic and international banking system. In addition, the Committee encourages the Secretary to consult with non-governmental ‘interested parties,’ including, for example, the Bank Secrecy Act Advisory Group, to obtain input from those who may be subject to a regulation or order under this section.

“Prior to invoking any of the special measures contained in section 5318A, the Secretary must consider three discrete factors, namely (1) whether other countries or multilateral groups have taken similar action; (2) whether the imposition of the measure would create a significant competitive disadvantage, including any significant cost or burden associated with compliance, for firms organized or licensed in the United States; and (3) the extent to which the action would have an adverse systemic impact on the payment system or legitimate

business transactions.

“Finally, subsection (a) makes clear that this new authority is not to be construed as superseding or restricting any other authority of the Secretary or any other agency.

“Subsection (b) of the new section 5318A outlines the five ‘special measures’ the Secretary may invoke against a foreign jurisdiction, financial institution operating outside the U.S., class of transaction within, or involving, a jurisdiction outside the U.S., or one or more types of accounts, that he finds to be of primary money laundering concern.

“The first such measure would require domestic financial institutions to maintain records and/or file reports on certain transactions involving the primary money laundering concern, to include any information the Secretary requires, such as the identity and address of participants in a transaction, the legal capacity in which the participant is acting, the beneficial ownership of the funds (in accordance with steps that the Secretary determines to be reasonable and practicable to obtain such information), and a description of the transaction. The records and/or reports authorized by this section must involve transactions from a foreign jurisdiction, a financial institution operating outside the United States, or class of international transactions within, or involving, a foreign jurisdiction, and are not to include transactions that both originate and terminate in, and only involve, domestic financial institutions.

“The second special measure would require domestic financial institutions to take such steps as the Secretary determines to be reasonable and practicable to ascertain beneficial ownership of accounts opened or maintained in the U.S. by a foreign person (excluding publicly traded foreign corporations) associated with what has been determined to be a primary money laundering concern.

“The third special measure the Secretary could impose in the case of a primary money laundering concern would require domestic financial institutions, as a condition of opening or maintaining a ‘payable-through account’ for a foreign financial institution, to identify each customer (and representative of the customer) who is permitted to use or whose transactions flow through such an account, and to obtain for each customer (and representative) information that is substantially comparable to the information it would obtain with respect to its own customers. A ‘payable-through account’ is defined for purposes of the legislation as an account, including a transaction account (as defined in section 19(b)(1)(C) of the Federal Reserve Act), opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a sub-account, in banking activities usual in connection with the business of banking in the United States.

“The fourth special measure the Secretary could impose in the case of a primary money laundering concern would require domestic financial institutions, as a condition of opening or maintaining a ‘correspondent’ account for a foreign financial institution, to identify each customer (and representative of the customer) who is permitted to use or whose transactions flow through such an account, and to obtain for each customer (and representative) information that is substantially comparable to the information that it would obtain with respect to its own customers. With respect to a bank, the term ‘correspondent account’ means an account established to receive deposits from and make payments on behalf of a foreign financial institution.

“The fifth measure the Secretary could impose in the case of a primary money laundering concern would prohibit or impose conditions (beyond those already provided for in the third and fourth measures) on domestic financial institutions’ correspondent or payable-through accounts with foreign banking institutions. In addition to the required consultation with the Chairman of the Board of Governors of the Federal Reserve, prior to imposing this measure the Secretary is also directed to consult with the Secretary of State and the Attorney General.

“The five special measures authorized by this section may be imposed in any sequence or combination as the Secretary determines. The first four special measures may be imposed

Due Diligence. Section 312 demands that all U.S. financial institutions have policies, procedures, and controls in place to identify instances where their correspondent and private banking accounts with foreign individuals and entities might be used for money laundering purposes, 31 U.S.C. 5318(i). They must establish enhanced due diligence standards for correspondent accounts held for offshore banking institutions (whose licenses prohibit them from conducting financial activities in the jurisdiction in which they are licensed) or institutions in money laundering jurisdictions designated by the Secretary of the Treasury or by international watch dog groups such as the Financial Action Task Force. The standards must at least involve reasonable efforts to identify the ownership of foreign institutions which are not publicly held; closely monitor the accounts for money laundering activity; and *to hold any foreign bank, for whom the U.S. institution has a correspondent account, to the same standards with respect to other correspondent accounts maintained by the foreign bank.* In the case of private banking accounts of \$1 million or more, U.S. financial institutions must keep records of the owners of the accounts and the source of funds deposited in the accounts. They must report suspicious transactions and, when the accounts are held for foreign officials, guard against transactions involving foreign official corruption.⁶³

by regulation, order, or otherwise as permitted by law. However, if the Secretary proceeds by issuing an order, the order must be accompanied by a notice of proposed rulemaking relating to the imposition of the special measure, and may not remain in effect for more than 120 days, except pursuant to a regulation prescribed on or before the end of the 120-day period. The fifth special measure may be imposed only by regulation,” H.R.Rep.No. 107-250, at 68-9.

⁶³ See generally, H.R.Rep.No. 107-250, at 71-2 (“Section [312] amends 31 U.S.C. 5318 to require financial institutions that establish, maintain, administer, or manage private banking or correspondent accounts for non-U.S. persons to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls to detect and report instances of money laundering through those accounts.

“The section requires financial institutions to apply enhanced due diligence procedures when opening or maintaining a correspondent account for a foreign bank operating (1) under a license to conduct banking activities which, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens of, or with the local currency of, the country which issued the license; or (2) under a license issued by a foreign country that has been designated (a) as non-cooperative with international anti-money laundering principles by an intergovernmental group or organization of which the United States is a member, with which designation the Secretary of the Treasury concurs, or (b) by the Secretary as warranting special measures due to money laundering concerns.

“The enhanced due diligence procedures include (1) ascertaining the identity of each of the owners of the foreign bank (except for banks that are publicly traded); (2) conducting enhanced scrutiny of the correspondent account to guard against money laundering and report any suspicious activity; and (3) ascertaining whether the foreign bank provides correspondent accounts to other foreign banks and, if so, the identity of those foreign banks and related due diligence information.

“For private banking accounts requested or maintained by a non-United States person, a financial institution is required to implement procedures for (1) ascertaining the identity of the nominal and beneficial owners of, and the source of funds deposited into, the account as needed to guard against money laundering and report suspicious activity; and (2) conducting enhanced scrutiny of any such account requested or maintained by, or on behalf of, a senior foreign political figure, or his immediate family members or close associates, to prevent,

General Regulatory Matters. The Act establishes several other regulatory mechanisms directed at the activities involving U.S. financial institutions and foreign individuals or institutions. Section 313, for instance, in another restriction on correspondent accounts for foreign financial institutions, prohibits U.S. financial institutions from maintaining correspondent accounts either directly or indirectly for foreign shell banks (banks with no physical place of business⁶⁴) which have no affiliation with any financial institution through which their banking activities are subject to regulatory supervision.⁶⁵

The Act, in section 325, empowers the Secretary of the Treasury to promulgate regulations to prevent financial institutions from allowing their customers to conceal their financial activities by taking advantage of the institutions' concentration account practices.⁶⁶

The Secretary of the Treasury is instructed in section 326 to issue regulations for financial institutions' minimum new customer identification standards and record-

detect and report transactions that may involve the proceeds of foreign corruption. A private bank account is defined as an account (or any combination of accounts) that requires a minimum aggregate deposit of funds or other assets of not less than \$1 million; is established on behalf of one or more individuals who have a direct or beneficial ownership in the account; and is assigned to, or administered or managed by, an officer, employee or agent of a financial institution acting as a liaison between the institution and the direct or beneficial owner of the account.

"This section directs the Secretary of the Treasury, within 6 months of enactment of this bill and in consultation with appropriate Federal functional regulators, to further define and clarify, by regulation, the requirements imposed by this section").

⁶⁴ Or more exactly, a bank which has no physical presence in any country; a "physical presence" for a foreign bank is defined as "a place of business that – (i) is maintained by a foreign bank; (ii) is located at a fixed address (other than solely an electronic address) in a country in which the foreign bank is authorized to conduct banking activities, at which location the foreign bank – (I) employs 1 or more individuals on a full-time basis; and (II) maintains operating records relating to its banking activities; and (iii) is subject to inspection by the banking authority which licensed the foreign bank to conduct banking activities," 31 U.S.C. 5318(j)(4).

⁶⁵ 31 U.S.C. 5318(j); H.R.Rep.No. 107-250, at 72 (2001).

⁶⁶ The Act does not define "concentration accounts," although the House Financial Services Committee report provides some insight into the section's intent, H.R.Rep.No. 107-250, at 72-3 (2001) ("This section gives the Secretary of the Treasury discretionary authority to prescribe regulations governing the maintenance of concentration accounts by financial institutions, to ensure that these accounts are not used to prevent association of the identity of an individual customer with the movement of funds of which the customer is the direct or beneficial owner. If promulgated, the regulations are required to prohibit financial institutions from allowing clients to direct transactions into, out of, or through the concentration accounts of the institution; prohibit financial institutions and their employees from informing customers of the existence of, or means of identifying, the concentration accounts of the institution; and to establish written procedures governing the documentation of all transactions involving a concentration account.")

keeping and to recommend a means to effectively verify the identification of foreign customers.⁶⁷

⁶⁷ 31 U.S.C. 5318(*l*); H.R.Rep.No. 107-250, at 62-3 (2001)(“Section [326](a) amends 31 U.S.C. 5318 by adding a new subsection governing the identification of account holders. Paragraph (1) directs Treasury to prescribe regulations setting forth minimum standards for customer identification by financial institutions in connection with the opening of an account. By referencing ‘customers’ in this section, the Committee intends that the regulations prescribed by Treasury take an approach similar to that of regulations promulgated under title V of the Gramm-Leach-Bliley Act of 1999, where the functional regulators defined ‘customers’ and ‘customer relationship’ for purposes of the financial privacy rules. Under this approach, for example, where a mutual fund sells its shares to the public through a broker-dealer and maintains a ‘street name’ or omnibus account in the broker-dealer’s name, the individual purchasers of the fund shares are customers of the broker-dealer, rather than the mutual fund. The mutual fund would not be required to ‘look through’ the broker-dealer to identify and verify the identities of those customers. Similarly, where a mutual fund sells its shares to a qualified retirement plan, the plan, and not its participants, would be the fund’s customers. Thus, the fund would not be required to ‘look through’ the plan to identify its participants.

“Paragraph (2) requires that the regulations must, at a minimum, require financial institutions to implement procedures to verify (to the extent reasonable and practicable) the identity of any person seeking to open an account, maintain records of the information used to do so, and consult applicable lists of known or suspected terrorists or terrorist organizations. The lists of known or suspected terrorists that the Committee intends financial institutions to consult are those already supplied to financial institutions by the Office of Foreign Asset Control (OFAC), and occasionally by law enforcement and regulatory authorities, as in the days immediately following the September 11, 2001, attacks on the World Trade Center and the Pentagon. It is the Committee’s intent that the verification procedures prescribed by Treasury make use of information currently obtained by most financial institutions in the account opening process. It is not the Committee’s intent for the regulations to require verification procedures that are prohibitively expensive or impractical.

“Paragraph (3) requires that Treasury consider the various types of accounts maintained by various financial institutions, the various methods of opening accounts, and the various types of identifying information available in promulgating its regulations. This would require Treasury to consider, for example, the feasibility of obtaining particular types of information for accounts opened through the mail, electronically, or in other situations where the accountholder is not physically present at the financial institution. Millions of Americans open accounts at mutual funds, broker-dealers, and other financial institutions in this manner; it is not the Committee’s intent that the regulations adopted pursuant to this legislation impose burdens that would make this prohibitively expensive or impractical. This provision allows Treasury to adopt regulations that are appropriately tailored to these types of accounts.

“Current regulatory guidance instructs depository institutions to make reasonable efforts to determine the true identity of all customers requesting an institution’s services. (See, e.g., FDIC Division of Supervision Manual of Exam Policies, section 9.4 VI.) The Committee intends that the regulations prescribed under this section adopt a similar approach, and impose requirements appropriate to the size, location, and type of business of an institution.

“Paragraph (4) requires that Treasury consult with the appropriate functional regulator in developing the regulations. This will help ensure that the regulations are appropriately tailored to the business practices of various types of financial institutions, and the risks that such practices may pose.

“Paragraph (5) gives each functional regulator the authority to exempt, by regulation or order, any financial institution or type of account from the regulations prescribed under paragraph (1).

Federal regulatory authorities must approve the merger of various financial institutions under the Bank Holding Company Act, 12 U.S.C. 1842, and the Federal Deposit Insurance Act, 12 U.S.C. 1828. Section 327 requires consideration of an institution's anti-money laundering record when such mergers are proposed, 12 U.S.C. 1842(c)(6), 1828(c)(11).

Section 314 directs the Secretary of the Treasury to promulgate regulations in order to encourage financial institutions and law enforcement agencies to share information concerning suspected money laundering and terrorist activities, 31 U.S.C. 5311 note.

Section 319(b) requires U.S. financial institutions to respond to bank regulatory authorities' requests for anti-money laundering records (within 120 hours) and to Justice or Treasury Department subpoenas or summons for records concerning foreign deposits (within 7 days), 31 U.S.C. 5318(k). Section 319 also calls for civil penalties of up to \$10,000 a day for financial institutions who have failed to terminate correspondent accounts with foreign institutions that have ignored Treasury or Justice Department subpoenas or summons, 31 U.S.C. 5318(k)(3).

Section 352 directs the Secretary of the Treasury to promulgate regulations, in consultation with other appropriate regulatory authorities, requiring financial institutions to maintain anti-money laundering programs which must include at least a compliance officer; an employee training program; the development of internal policies, procedures and controls; and an independent audit feature.⁶⁸

Section 359 subjects money transmitters to the regulations and requirements of the Currency and Foreign Transactions Reporting Act (31 U.S.C. 5311 et seq.) and directs the Secretary of the Treasury to report on the need for additional legislation relating to domestic and international underground banking systems.

Federal law obligates the Administration to develop a national strategy for combating money laundering and related financial crimes, 31 U.S.C. 5341. Section 354 insists that the strategy contain data relating to the funding of international terrorism and efforts to prevent, detect, and prosecute such funding, 31 U.S.C. 5341(b)(12).

Section 364 authorizes the Board of Governors of the Federal Reserve to hire guards to protect members of the Board, as well as the Board's property and personnel and that of any Federal Reserve bank. The guards may carry firearms and make arrests, 12 U.S.C. 248(q).

Reports to Congress. Section 366 instructs the Secretary of the Treasury to report on methods of improving the compliance of financial institutions with the currency transaction reporting requirements and on the possibility of expanding

"Paragraph (6) requires that Treasury's regulations prescribed under paragraph (1) become effective within one year after enactment of this bill").

⁶⁸ 31 U.S.C. 5318(h); H.R.Rep.No. 107-250, at 72 (2001).

exemptions to the requirements with an eye to improving the quality of data available for law enforcement purposes and reducing the number of unnecessary filings.⁶⁹

Section 324 instructs the Secretary of the Treasury to report on the execution of authority granted under the International Counter Money Laundering and Related Measures subtitle (III-A) of the Act and to recommend any appropriate related legislation, 31 U.S.C. 5311 note.

International Cooperation. Reflecting concern about the ability of law enforcement officials to trace money transfers to this country from overseas, section 328 instructs the Secretary of the Treasury, Secretary of State and Attorney General to make every effort to encourage other governments to require identification of the originator of international wire transfers.⁷⁰

Section 330 expresses the sense of the Congress that the Administration should seek to negotiate international agreements to enable U.S. law enforcement officials to track the financial activities of foreign terrorist organizations, money launderers and other criminals.

Section 360 authorizes the Secretary of the Treasury to direct the U.S. Executive Directors of the various international financial institutions (*i.e.*, the International Monetary Fund, the International Bank for Reconstruction and Development, the European Bank for Reconstruction and Development, the International Development Association, the International Finance Corporation, the Multilateral Investment Guarantee Agency, the African Development Bank, the African Development Fund, the Asian Development Bank, the Bank for Economic Development and Cooperation in the Middle East and North Africa, and the InterAmerican Investment Corporation): (1) to support the loan and other benefit efforts on behalf of countries that the President determines have supported our anti-terrorism efforts, and (2) to vote to ensure that funds from those institutions are not used to support terrorism.

⁶⁹ 31 U.S.C. 5313 note; H.R.Rep.No. 107-205, at 65 (2001).

⁷⁰ H.R.Rep.No. 107-250, at 67 (2001) (“This section directs the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to (1) take all reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the U.S. and other countries; and (2) report annually to Congress on Treasury’s progress in achieving this objective, and on impediments to instituting a regime in which all appropriate identification about wire transfer recipients is included with wire transfers from their point of origination until disbursement.

“The Committee is concerned that inadequate information on the originator of wire transfers from a number of foreign jurisdictions makes it difficult for both law enforcement and financial institutions to properly understand the source of funds entering the United States in wire transfers. Such a lack of clarity could aid money launderers or terrorists in moving their funds into the United States financial system. Additionally, while arguments have been made that there are technical impediments to requiring that complete addressee information appear on all wire transfers terminating in or passing through the United States, the Committee believes that having such information is technically feasible and would aid both financial institutions in performing due diligence and law enforcement in tracking or seizing money that is the derivative of or would be used in the commission of a crime”).

Crimes. Federal criminal money laundering statutes punish both concealing the fruits of old offenses and financing new ones. They proscribe financial transactions which:

- involve more than \$10,000 derived from one of a list of specified underlying crimes, 18 U.S.C. 1957, or
- are intended to promote any of the designated predicate offenses, or
- are intended to evade taxes, or
- are designed to conceal the proceeds generated by any of the predicate offenses, or
- are crafted to avoid transaction reporting requirements, 18 U.S.C. 1956.

They also condemn transporting funds into, out of, or through the United States with the intent to further a predicate offense, conceal its proceeds, or evade reporting requirements, 18 U.S.C. 1956. Offenders face imprisonment for up to twenty years, fines of up to \$500,000, civil penalties, 18 U.S.C. 1956, 1957, and confiscation of the illicit funds involved in a violation or in any of the predicate offenses, 18 U.S.C. 981, 982.

The Act contains a number of new money laundering crimes, as well as amendments and increased penalties for existing crimes. Section 315, for example, adds several crimes to the federal money laundering predicate offense list of 18 U.S.C. 1956. The newly added predicate offenses include crimes in violation of the laws of the other nations when the proceeds are involved in financial transactions in this country: crimes of violence, public corruption, smuggling, and offenses condemned in treaties to which we are a party, 18 U.S.C. 1956(c)(7)(B). Additional federal crimes also join the predicate list:

- 18 U.S.C. 541 (goods falsely classified)
- 18 U.S.C. 922(1) (unlawful importation of firearms)
- 18 U.S.C. 924(n) (firearms trafficking)
- 18 U.S.C. 1030 (computer fraud and abuse)
- felony violations of the Foreign Agents Registration Act, 22 U.S.C. 618.

As the report accompanying H.R. 3004 explains:

This amendment enlarges the list of foreign crimes that can lead to money laundering prosecutions in this country when the proceeds of additional foreign crimes are laundered in the United States. The additional crimes include all crimes of violence, public corruption, and offenses covered by existing bilateral extradition treaties. The Committee intends this provision to send a strong signal that the United States will not tolerate the use of its financial institutions for the purpose of laundering the proceeds of such activities. H.R.Rep.No. 107-250, at 55 (2000).

In this same vein, section 376 adds the crime of providing material support to a terrorist organization (18 U.S.C. 2339B) to the predicate offense list and section 318

expands 18 U.S.C. 1956 to cover financial transactions conducted in foreign financial institutions.⁷¹

Section 329 makes it a federal crime to corruptly administer the money laundering regulatory scheme. Offenders are punishable by imprisonment for not more than 15 years and a fine of not more than three times the amount of the bribe.

Section 5326 of title 31 authorizes the Secretary of the Treasury to impose temporary, enhanced reporting requirements upon financial institutions in areas victimized by substantial money laundering activity (geographic targeting regulations and orders). Section 353 makes it clear that the civil sanctions, criminal penalties, and prohibitions on smurfing (structuring transactions to evade reporting requirements) apply to violations of the regulations and orders issued under 31 U.S.C. 5326.⁷² It also extends the permissible length of the temporary geographical orders from 60 to 180 days.

Violations of the special measures and special due diligence requirements of sections 311 and 312 are subject to both civil and criminal penalties by virtue of section 363's amendments to 31 U.S.C. 5321(a) and 5322. The amendments authorize civil penalties and criminal fines of twice the amount of the transaction but not more than \$1 million. Criminal offenders would be subject to a fine in the same amount.

⁷¹ “[S]ection 1956 of title 18, United States Code, makes it an offense to conduct a transaction involving a financial institution if the transaction involves criminally derived property. Similarly, 18 U.S.C. 1957 creates an offense relating to the deposit, withdrawal, transfer or exchange of criminally derived funds ‘by, to or through a financial institution.’ For the purposes of both statutes, the term ‘financial institution’ is defined in 31 U.S.C. 5312. See 18 U.S.C. 1956(c)(6); 18 U.S.C. 1957(f).

“The definition of ‘financial institution’ in 5312 does not explicitly include foreign banks. Such banks may well be covered because they fall within the meaning of ‘commercial bank’ or other terms in the statute, but as presently drafted, there is some confusion over whether the government can rely on section 5312 to prosecute an offense under either 1956 or 1957 involving a transaction through a foreign bank, even if the offense occurs in part in the United States. For example, if a person in the United States sends criminal proceeds abroad--say to a Mexican bank--and launders them through a series of financial transactions, the government conceivably could not rely on the definition of a ‘financial institution’ in 1956(c)(6) to establish that the transaction was a ‘financial transaction’ within the meaning of 1956(c)(4)(B) (defining a ‘financial transaction’ as a transaction involving the use of a ‘financial institution’), or that it was a ‘monetary transaction’ within the meaning of 1957(f) (defining ‘monetary transaction’ as, inter alia, a transaction that would be a ‘financial transaction’ under 1956(c)(4)(B)).

“Similarly, the money laundering laws in effect in most countries simply make it an offense to launder the proceeds of any crime, foreign or domestic. In the United States, however, the money laundering statute is violated only when a person launders the proceeds of one of the crimes set forth on a list of ‘specified unlawful activities.’ 18 U.S.C. 1956(c)(7). Currently only a handful of foreign crimes appear on that list. See 1956(c)(7)(B),” H.R.Rep.No. 107-250, at 38 (2000).

⁷² Cf., H.R.Rep.No. 107-250, at 57.

Earlier federal law prohibited the operation of illegal money transmitting businesses, 18 U.S.C. 1960. Section 373 amends the proscription to make it clear that the prohibition must be breached “knowingly” and to cover businesses which are otherwise lawful but which transmit funds they know are derived from or intended for illegal activities. It also amends 18 U.S.C. 981(a)(1)(A) to permit civil forfeiture of property involved in a transaction in violation of 18 U.S.C. 1960.⁷³

Sections 374 and 375 of the Act seek to curtail economic terrorism by increasing and making more uniform the penalties for counterfeiting U.S. or foreign currency and by making it clear that the prohibitions against possession of counterfeiting paraphernalia extend to their electronic equivalents.⁷⁴ They increase the maximum terms of imprisonment for violation of:

- 18 U.S.C. 471 (obligations or securities of the U.S.) from 15 to 20 years;
- 18 U.S.C. 472 (uttering counterfeit obligations and securities) from 15 to 20 years;
- 18 U.S.C. 473 (dealing in counterfeit obligations and securities) from 10 to 20 years;

⁷³ “The operation of an unlicensed money transmitting business is a violation of Federal law under 18 U.S.C. 1960. First, section 104 clarifies the scienter requirement in 1960 to avoid the problems that occurred when the Supreme Court interpreted the currency transaction reporting statutes to require proof that the defendant knew that structuring a cash transaction to avoid the reporting requirements had been made a criminal offense. See *Ratzlaf v. United States*, 114 S. Ct. 655 (1994). The proposal makes clear that an offense under 1960 is a general intent crime for which a defendant is liable if he knowingly operates an unlicensed money transmitting business. For purposes of a criminal prosecution, the Government would not have to show that the defendant knew that a State license was required or that the Federal registration requirements promulgated pursuant to 31 U.S.C. 5330 applied to the business.

“Second, section 104 expands the definition of an unlicensed money transmitting business to include a business engaged in the transportation or transmission of funds that the defendant knows are derived from a criminal offense, or are intended to be used for an unlawful purpose. Thus, a person who agrees to transmit or to transport drug proceeds for a drug dealer, or funds from any source for a terrorist, knowing such funds are to be used to commit a terrorist act, would be engaged in the operation of an unlicensed money transmitting business. It would not be necessary for the Government to show that the business was a storefront or other formal business open to walk-in trade. To the contrary, it would be sufficient to show that the defendant offered his services as a money transmitter to another.

“Finally, when Congress enacted 1960 in 1992, it provided for criminal but not civil forfeiture. The proposal corrects this oversight, and allows the government to obtain forfeiture of property involved in the operation of an illegal money transmitting business even if the perpetrator is a fugitive,” H.R.Rep.No. 107-250, at 54 (2001).

⁷⁴ “This section makes it a criminal offense to possess an electronic image of an obligation or security document of the United States with intent to defraud. The provision harmonizes counterfeiting language to clarify that possessing either analog or digital copies with intent to defraud constitutes an offense. This section mimics existing language that makes it a felony to possess the plates from which currency can be printed, and takes into account the fact that most counterfeit currency seized today is generated by computers or computer-based equipment. The section also increases maximum sentences for a series of counterfeiting offenses,” H.R.Rep.No. 107-250, at 75-6 (2001).

- 18 U.S.C. 476 (taking impressions of tools used for obligations and securities) from 10 to 25 years;
- 18 U.S.C. 477 (possessing or selling impressions of tools used for obligations or securities) from 10 to 25 years;
- 18 U.S.C. 484 (connecting parts of different notes) from 5 to 10 years;
- 18 U.S.C. 493 (bonds and obligations of certain lending agencies) from 5 to 10 years;
- 18 U.S.C. 478 (foreign obligations or securities) from 5 to 20 years;
- 18 U.S.C. 479 (uttering counterfeit foreign obligations or securities) from 3 to 20 years;
- 18 U.S.C. 480 (possessing counterfeit foreign obligations or securities) from 1 to 20 years;
- 18 U.S.C. 481 (plates, stones, or analog, digital, or electronic images for counterfeiting foreign obligations or securities) from 5 to 25 years;
- 18 U.S.C. 482 (foreign bank notes) from 2 to 20 years; and
- 18 U.S.C. 483 (uttering counterfeit foreign bank notes) from 1 to 20 years.

Aliens believed to have engaged in money laundering may not enter the United States, section 1006 (8 U.S.C. 1182(a)(2)(I)). The same section directs the Secretary of State to maintain a watchlist to ensure that they are not admitted, 8 U.S.C. 1182 note.

Bulk Cash. Customs officials ask travelers leaving the United States whether they are taking \$10,000 or more in cash with them. Section 1001 of title 18 of the United States Code makes a false response punishable by imprisonment for not more than 5 years. Section 5322 of title 31 makes failure to report taking \$10,000 or more to or from the United States punishable by the same penalties. The Act's bulk cash smuggling offense, section 371, augments these proscriptions with a somewhat unique feature, 31 U.S.C. 5332 – a criminal forfeiture of the smuggled cash in lieu of a criminal fine. The basic offense outlaws smuggling cash into or out of the United States. The concealment element of the offense seems to cover everything but in-sight possession as long as an amount \$10,000 or more is carried in manner to evade reporting.⁷⁵

The section appears to be the product of reactions to the Supreme Court's decision in *United States v. Bajakian*, 524 U.S. 321 (1998). There officials had confiscated \$350,000 because Bajakian attempted to leave the country without declaring it, a violation of 31 U.S.C. 5322. In the view of the Court, the confiscation was grossly disproportionate to the gravity of the offense and consequently contrary to the Constitution's excessive fines clause, 524 U.S. at 337. The Committee Report accompanying H.R. 3004 explains the Justice Department's assurance that casting surreptitious removal of cash from the United States as a smuggling rather than a false reporting offense will avoid the adverse consequences of the Supreme Court's

⁷⁵ "For purposes of this section, the concealment of currency on the person of any individual includes concealment in any article of clothing worn by the individual or in any luggage, backpack, or other container worn or carried by such individual," 31 U.S.C. 5332(a)(2).

examination of forfeiture in false reporting cases under the Constitution's Excessive Fines Clause.⁷⁶

Section 5317 of title 31 once called for civil forfeiture of property traceable to a violation of 31 U.S.C. 5316 (reports on exporting or importing money instruments worth \$10,000 or more). Section 372 of the Act recasts section 5317 to provide for civil and criminal forfeitures for violations of 31 U.S.C. 5316, of 31 U.S.C. 5313 (reports on domestic coins and currency transactions involving \$10,000 or more) and of 31 U.S.C. 5324 (structuring transactions to evade reporting requirements (smurfing)).

Extraterritorial Jurisdiction. The Act makes 18 U.S.C. 1029, the federal statute condemning various crimes involving credit cards, PIN numbers and other access devices, applicable overseas if the card or device is issued by or controlled by an American bank or other entity *and* some article is held in or transported to or through the United States during the course of the offense, section 377. The change was part of the original Justice Department proposals. Justice explained that, “[financial crime[] admits of no border, utilizing the integrated global financial network for ill purposes. This provision would apply the financial crimes prohibitions to conduct committed abroad, so long as the tools or proceeds of the crimes pass through or are in the United States,” *DoJ* at §408. The section, however, appears to limit the otherwise applicable extraterritorial jurisdiction implicit in section 1029, since federal courts would likely recognize extraterritorial jurisdiction over a violation

⁷⁶ “As recent Congressional hearings have demonstrated, currency smuggling is an extremely serious law enforcement problem. Hundreds of millions of dollars in U.S. currency – representing the proceeds of drug trafficking and other criminal offenses – is annually transported out of the United States to foreign countries in shipments of bulk cash. Smugglers use all available means to transport the currency out of the country, from false bottoms in personal luggage, to secret compartments in automobiles, to concealment in durable goods exported for sale abroad. . . .

“Presently, the only law enforcement weapon against such smuggling is section 5316 of title 31, United States Code, which makes it an offense to transport more than \$10,000 in currency or monetary instruments into, or out of, the United State without filing a report with the United States Customs Service. The effectiveness of section 5316 as a law enforcement tool has been diminished, however, by a recent Supreme Court decision. In *United States v. Bajakajian*, 118 S.Ct. 2028 (1998), the Supreme Court held that section 5316 constitutes a mere reporting violation, which is not a serious offense for purposes of the Excessive Fines Clause of the Eighth Amendment. Accordingly, confiscation of the full amount of the smuggled currency is unconstitutional, even if the smuggler took elaborate steps to conceal the currency and otherwise obstruct justice.

“Confiscation of the smuggled currency is, of course, the most effective weapon that can be employed against currency smugglers. Accordingly, in response to the *Bajakajian* decision, the Department of Justice proposed making the act of bulk cash smuggling itself a criminal offense, and to authorize the imposition of the full range of civil and criminal sanctions when the offense is discovered. Because the act of concealing currency for the purpose of smuggling it out of the United States is inherently more serious than simply failing to file a customs report, strong and meaningful sanctions, such as confiscation of the smuggled currency, are likely to withstand Eighth Amendment challenges to the new statute,” H.R.Rep.No. 107-250 at 36-7 (2001).

under *either* circumstance (issued by a U.S. entity or physical presence in the U.S.) as well as a number of others.⁷⁷

Venue. Section 1004 relies on *dicta* in *United States v. Cabrales*, 524 U.S. 1, 8 (1998), in order to permit a money laundering prosecution to be brought in the place where the crime which generated the funds occurred, “if the defendant participated in the transfer of the proceeds,” 18 U.S.C. 1956(i).

Ordinarily, the Constitution requires that a crime be prosecuted in the state and district in which it occurs, in the case of money laundering,⁷⁸ in the state and district in which the monetary transaction takes place. The Supreme Court in *Cabrales* held that a charge of money laundering in Florida, of the proceeds of a Missouri drug trafficking, could not be tried in Missouri. The Court declared in *dicta*, however, that “money laundering . . . arguably might rank as a continuing offense, triable in more than one place, if the launderer acquired the funds in one district and transported them into another,” 524 U.S. at 8.⁷⁹

Forfeiture. Forfeiture is the government confiscation of property as a consequence of crime.⁸⁰ The forfeiture amendments of the Act fall into two categories. Some make adjustments to those portions of federal forfeiture law which govern the confiscation of property derived from, or used to facilitate, various federal crimes. Others follow the pattern used for the war-time confiscation of the property of enemy aliens under the Trading With the Enemy Act, 50 U.S.C.App. 1 *et seq.* (TWEA), forfeitures which turn on the ownership of the property rather than upon its proximity to any particular crime.

Constitutional Considerations. The Act adds TWEA-like amendments to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701 *et seq.*, which already allowed the President to freeze the assets of foreign terrorists under certain conditions. Under IEEPA, as amended by section 106 of the Act, the President or his delegate may confiscate and dispose of any property, within the

⁷⁷ *United States v. Bowman*, 260 U.S. 94, 97-8 (1922); *Ford v. United States*, 273 U.S. 593, 623 (1927). For a general discussion of the extraterritorial application of federal criminal law, see, Doyle, *Extraterritorial Application of American Criminal Law*, CRS REP.NO. 94-166A (Mar. 13, 1999).

⁷⁸ “The trial of all crimes . . . shall be held in the state where the said crimes shall have been committed; but when not committed within any state, the trial shall be at such place or places as the Congress may by law have directed,” *U.S. Const.* Art.III, §2, cl.3.

“[I]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed; which district shall have been previously ascertained by law,” *U.S. Const.* Amend. VI.

⁷⁹ See also, *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280-81 n.4 (1999) (holding that acquiring and using a firearm in Maryland in connection with a kidnaping in New Jersey might constitutionally be prosecuted in New Jersey under a statute which outlawed possession of a firearm “during and in relation to” a crime of violence.

⁸⁰ For general background information, see, Doyle, *Crime and Forfeiture*, CRS REP.NO. 97-139A (Oct. 11, 2000).

jurisdiction of the United States, belonging to any foreign individual, foreign entity, or foreign country whom they determine to have planned, authorized, aided or engaged in an attack on the United States by a foreign country or foreign nationals. The section also permits the government to present secretly (*ex parte* and *in camera*) any classified information upon which the forfeiture was based should the decision be subject to judicial review. The Justice Department requested the section as a revival of the President's powers in times of unconventional wars.⁸¹ By virtue of section 316, property owners may initiate a challenge to a confiscation by filing a claim under the rules applicable in maritime confiscations. The section permits two defenses to forfeiture – that the property is not subject to confiscation under section 106 or that the claimant is entitled to the innocent owner defense of 18 U.S.C. 983(d).⁸² The characterization of the defenses as “affirmative defense” indicates that the claimant *bears the burden of proof*. *The innocent owner defenses of 18 U.S.C. 983(d) are probably not available in cases under section 106, since that section is explicitly*

⁸¹ “This section is designed to accomplish two principal objectives. First, the section restores to the President, in limited circumstances involving armed hostilities or attacks against the United States, the power to confiscate and vest in the United States property of enemies during times of national emergency, which was contained in the Trading with the Enemy Act, 50 App. U.S.C. §5(b)(TWEA) until 1977. Until the International Economic Emergency Act (IEEPA) was passed in 1977, section 5(b) permitted the President to vest enemy property in the United States during time of war *or* national emergency. When IEEPA was passed, it did not expressly include a provision permitting the vesting of property in the United States, and section 5(b) of TWEA was amended to apply only ‘during the time of war.’ 50 App.U.S.C. §5(b).

“This new provision tracks the vesting language currently in section 5(b) of TWEA and permits the President, only in the limited circumstances when the United States is engaged in military hostilities or has been subject to an attack, to confiscate property of any foreign country, person, or organization involved in hostilities or attacks on the United States. Like the original provision in TWEA, it is an exercise of Congress's war power under Article I, section 8, clause 11 of the Constitution and is designed to apply to unconventional warfare where Congress has not formally declared war against a foreign nation.

“The second principal purpose of this amendment to IEEPA is to ensure that reviewing courts may base their rulings on an examination of the complete administrative record in sensitive national security or terrorism cases without requiring the United States to compromise classified information. New section (c) would authorize a reviewing court, in the process of verifying that determinations made by the executive branch were based upon substantial evidence and were not arbitrary or capricious, to consider classified evidence *ex parte* and *in camera*. This would ensure that reviewing courts have the best and most complete information upon which to base their decisions without forcing the United States to choose between compromising highly sensitive intelligence information or declining to take action against individuals or entities that may present a serious threat to the United States or its nationals. A similar accommodation mechanism was enacted by Congress in the Anti-Terrorism and Effective Death Penalty Act of 1996, 8 U.S.C. §1189(b)(2),” *DoJ* at §159.

⁸² “An owner of property that is confiscated under any provision of law relating to the confiscation of assets of suspected international terrorists, may contest that confiscation by filing a claim in the manner set forth in the Federal Rules of Civil Procedure (Supplemental Rules for Certain Admiralty and Maritime Claims), and asserting as an affirmative defense that – (1) the property is not subject to confiscation under such provision of law; or (2) the innocent owner provisions of section 983(d) of title 18, United States Code, apply to the case,” Sec. 316(a).

excepted from the coverage of 18 U.S.C. 983.⁸³ The challenge proceedings permit the court to admit evidence, such as hearsay evidence, that would not otherwise be admissible under the Federal Rules of Evidence if the evidence is reliable and if national security might be imperiled should dictates of the Federal Rules be followed, §316(b). The section recognizes the rights of claimants to proceed alternatively under the Constitution or the Administrative Procedure Act.⁸⁴

The Justice Department also recommended enactment of an overlapping provision which ultimately passed as section 806 of the Act without any real discussion of the relationship of the two sections.⁸⁵ Section 806 authorizes confiscation of all property, regardless of where it is found, of any individual, entity, or organization engaged in domestic or international terrorism (as defined in 18 U.S.C. 2331),⁸⁶ against the United States, Americans or their property, 18 U.S.C.

⁸³ 18 U.S.C. 983(i)(2)(D).

⁸⁴ “The exclusion of certain provisions of Federal law from the definition of the term ‘civil forfeiture statute’ in section 983(i) of title 18, United States Code, shall not be construed to deny an owner of property the right to contest the confiscation of assets of suspected international terrorists under – (A) subsection (a) of this section; (B) the Constitution; or (C) subchapter II of chapter 5 of title 5, United States Code (commonly known as the ‘Administrative Procedure Act’),” Sec. 316(c)(1).

⁸⁵ “Current law does not contain any authority tailored specifically to the confiscation of terrorist assets. Instead, currently, forfeiture is authorized only in narrow circumstances for the proceeds of murder, arson, and some terrorism offenses, or for laundering the proceeds of such offenses. However, most terrorism offenses do not yield ‘proceeds,’ and available current forfeiture laws require detailed tracing that is quite difficult for accounts coming through the banks of countries used by many terrorists.

“This section increases the government’s ability to strike at terrorist organizations’ economic base by permitting the forfeiture of its property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense. This is similar in concept to the forfeiture now available under RICO. In parity with the drug forfeiture laws, the section also authorizes the forfeiture of property used or intended to be used to facilitate a terrorist act, regardless of its source. There is no need for a separate criminal forfeiture provision because criminal forfeiture is incorporated under current law by reference. The provision is retroactive to permit it to be applied to the events of September 11, 2001,” *DoJ*, at §403. The House Report on H.R. 2975 which contained versions of both sections is no more explicit on the relation of the two sections.

⁸⁶ “(1) the term ‘international terrorism’ means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . (5) the term ‘domestic terrorism’ means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct

981(a)(1)(G). Section 806 as discussed below also calls for the more common confiscation of property derived from and or facilitating acts of domestic or international terrorism against the United States or its citizens. Confiscations under 806 may be challenged under the procedures of 18 U.S.C. 983, since they are not exempted there. To the extent that forfeiture under section 806 is based on international rather than domestic terrorism, claimants may also use the procedures of section 316.

Confiscation based solely on the fact that the property is owned by a criminal offender, rather than that it is derived from or facilitates some crime is fairly uncommon. It is the mark of common law forfeiture of estate. At common law, a felon forfeited all of his property. Most contemporary forfeiture statutes employ statutory forfeiture, a more familiar presence in American law,⁸⁷ which consists of the confiscation of things whose possession is criminal, of the fruits of crime, and of the means of crime – untaxed whiskey, the drug dealer’s profits, and the rum runner’s ship.

Three characteristics set forfeiture of estate apart. The property is lost solely by reason of its ownership by a felon. All of a felon’s property is confiscated, not merely that which is related to the crime for which he is convicted. Finally, it occasions attainder which negates the felon’s right to hold property or for title to property to pass through him to his heirs. It was with this in mind, that the Framers declared that “no attainder of treason shall work corruption of blood or forfeiture exception during the life of the person attainted.”⁸⁸ And for this reason, President Lincoln insisted that the confiscated real estate of Confederate supporters should revert their heirs at death.⁸⁹

of a government by mass destruction, assassination or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States,” 18 U.S.C. 2331(1),(5)(as amended by section 802 of the Act).

⁸⁷ *Austin v. United States*, 509 U.S. 602, 611-12 (1993)(“Three kinds of forfeiture were established in England at the time the Eighth Amendment was ratified in the United States: deodand, forfeiture, and statutory forfeiture Of England’s three kinds of forfeiture, only the third took hold in the United States”).

⁸⁸ *U.S. Const.* Art.III, §3, cl.2.

⁸⁹ 12 Stat. 589, 627 (1862). Some would suggest a fourth distinction: that it follows a felony conviction. This is hardly a distinction, since over time legislation creating statutory forfeitures has employed criminal *in personam* proceedings following criminal conviction as a means of accomplishing confiscation.

Neither section 106 nor 806 require conviction of the terrorist property owner.⁹⁰ Both call for forfeiture of all of the terrorist's property, without requiring any nexus to the terrorist's offenses other than terrorist ownership. Neither makes any explicit provision for the terrorist's heirs. Section 106 applies only to foreign persons, organizations, or countries, but section 806 recognizes no such distinction.

Of course, the Supreme Court long ago confirmed the constitutional validity of a seemingly similar pattern in TWEA under the President's war powers.⁹¹ The Court was careful to point out, however, that the TWEA procedure was not really forfeiture or confiscation for the benefit of the United States, but by express statutory provision a liquidation measure to protect the creditors of enemy property owners.⁹² Neither section 106 nor 806 are part of TWEA and neither explicitly treats the proceeds of confiscation as a fund for the benefit of creditors. Moreover, broad as the President's war powers may be, they would hardly seem to provide a justification for section 806, which embraces domestic terrorism and is neither limited to foreign offenders nor predicated upon war-like hostilities.

Criminal forfeitures, civil forfeitures with punitive as well as remedial purposes, and civil forfeitures whose effect is so punitive as to negate any presumption of remedial purpose, all raise other constitutional points of interest. The Eighth Amendment's excessive fines clause prohibits criminal forfeitures, and civil forfeitures with at least some punitive purposes, that are grossly disproportionate to the gravity of the crimes which trigger them.⁹³ The Fifth Amendment's double jeopardy clause applies to criminal forfeitures and civil forfeitures which are so punitive as to negate

⁹⁰ Although by operation of law property subject to civil forfeiture of section 806 may be confiscated upon conviction of the property owner for any crime of domestic or international terrorism, 28 U.S.C. 2461(c) ("If a forfeiture of property is authorized in connection with a violation of an Act of Congress, and any person is charged in an indictment or information with such violation but no specific statutory provision is made for criminal forfeiture upon conviction, the Government may include the forfeiture in the indictment or information in accordance with the Federal Rules of Criminal Procedure, and upon conviction, the court shall order the forfeiture of the property in accordance with the procedures set forth in section 413 of the Controlled Substances Act").

⁹¹ *Silesian American Corp. V. Clark*, 332 U.S. 469 (1947); *cf.*, *Societe Internationale v. Rogers*, 357 U.S. 197, 211 (1958) ("this summary power to seize property which is believed to be enemy-owned is rescued from constitutional invalidity under the Due Process and Just Compensation Clauses of the Fifth Amendment only by those provisions of the Act which afford a non-enemy claimant a later judicial hearing as to the propriety of the seizure").

⁹² *Zittman v. McGrath*, 341 U.S. 471, 473-74 (1951) (citing 50 U.S.C.App. 34) ("While the statute under which the funds are to be 'held, administered and accounted for' authorizes the vesting of such foreign-owned property in the custodian and its administration 'in the interest of and for the benefit of the United States,' it is not a confiscation measure, but a liquidation measure for the protection of American creditors. It provides for the filing and proving of claims and states that the funds 'shall be equitably applied for the payments of debts').

⁹³ *United States v. Bajakajian*, 524 U.S. 321, 337 (1998); *Austin v. United States*, 509 U.S. 602, 622 (1993).

any presumption of remedial purposes.⁹⁴ The same has been said of the applicability of the ex post facto clause.⁹⁵

The limitations on criminal forfeitures would apply to the forfeitures under section 806 when prosecuted as criminal forfeitures by operation of 28 U.S.C. 2461(c). The offenses that activate section 106 and 806 confiscations, however, are of such gravity that successful excessive fine clause challenges are unlikely, even if the value of confiscated property were extraordinarily high.

On the other hand, there is more than a little support for the argument that section 106 and 806 constitute punitive rather than remedial measures. They are potentially severe. Section 806 calls for the total impoverishment of those to whom it applies (all assets foreign and domestic), while section 106 anticipates confiscation of all assets within the jurisdiction of the United States. They seem to undermine any claim to remedial purpose by reaching those assets that neither facilitate the commission of terrorism nor constitute its fruits. Moreover, in its analysis of the language of section 806, the Justice Department described it as conceptually akin to the criminal forfeiture provisions of RICO.⁹⁶ If the courts find section 106 or 806 are civil in name but criminal in nature, they may well conclude that efforts to enforce the sections are bound by the limitations of the double jeopardy and ex post facto clauses.

Other Forfeiture Amendments. In order to more effectively enforce money laundering penalties and prosecute civil forfeiture actions involving foreign individuals or entities, section 317 of the Act establishes a procedure for long-arm jurisdiction over individuals and entities located overseas and for the appointment of a federal receiver to take control of contested assets during the pendency of the proceedings.⁹⁷

⁹⁴ *United States v. Ursery*, 518 U.S. 267, 278 (1996).

⁹⁵ See e.g., *United States v. Certain Funds (Hong Kong and Shanghai Banking Corp.)*, 96 F.3d 20, 26-7 (2d Cir. 1996). Where the ex post facto clauses do not apply, the validity of retroactive statutes is judged by due process clause standards. There is a presumption against retroactive application in such instances absent a clear indication of contrary Congressional intent grounded in the view that due process demands certain minimal notice of the law's demands, *Landgraf v. USI Film Products*, 511 U.S. 244, 265-66 (1994).

⁹⁶ *DoJ*, at §403.

⁹⁷ 18 U.S.C. 1956(b). Cf., H.R.Rep.No. 107-250, at 54-5 (2001) ("The first provision in this section creates a long arm statute that gives the district court jurisdiction over a foreign person, including a foreign bank, that commits a money laundering offense in the United States or converts laundered funds that have been forfeited to the Government to his own use. Thus, if the Government files a civil enforcement action under section 1956(b), or files a civil lawsuit to recover forfeited property from a third party, the district court would have jurisdiction over the defendant if the defendant has been served with process pursuant to the applicable statutes or rules of procedure, and the constitutional requirement of minimum contacts is satisfied in one of three ways: the money laundering offense took place in the United States; in the case of converted property, the property was the property of the United States by virtue of a civil or criminal forfeiture judgment; or in the case of a financial institution, the defendant maintained a correspondent bank account at another bank in the United States. Under this provision, for example, the district courts would have had jurisdiction over the defendant in the circumstances described in *United States v. Swiss*

In the case of inter-bank accounts where a bank in a foreign nation has an account in a bank located in the United States, section 319(a) allows seizure of funds in an account here when the foreign bank has received money laundering or drug trafficking deposits overseas.⁹⁸ Confiscation proceedings are conducted pursuant to 18 U.S.C. 953.

Federal law has for some time permitted criminal forfeiture orders to reach substitute assets if the property of the defendant subject to confiscation has become unavailable. Section 319(d) establishes a procedure under which a convicted

American Bank, 191 F.3d 30 (1st Cir. 1999).

“The second provision, modeled on 18 U.S.C. 1345(b), gives the district court the power to restrain property, issue seizure warrants, or take other action necessary to ensure that a defendant in an action covered by the statute does not dissipate the assets that would be needed to satisfy a judgment.

“This section also authorizes a court, on the motion of the Government or a State or Federal regulator, to appoint a receiver to gather and protect assets needed to satisfy a judgment under sections 1956 and 1957, and the forfeiture provisions in sections 981 and 982. This authority is intended to apply in three circumstances: (1) when there is a judgment in a criminal case, including an order of restitution, following a conviction for a violation of section 1956 or 1957; (2) when there is a judgment in a civil case under section 1956(b) assessing a penalty for a violation of either section 1956 or 1957; and (3) when there is a civil forfeiture judgment under section 981 or a criminal forfeiture judgment, including a personal money judgment, under section 982.

“The amendment also makes section 1956(b) applicable to violations of section 1957. It applies to conduct occurring before the effective date of the Act”).

⁹⁸ 18 U.S.C. 981(k). H.R.Rep.No. 107-250, at 57-8 (2001)(“Section 114 creates a new provision in the civil forfeiture statute, 18 U.S.C. 981(k), authorizing the forfeiture of funds found in an interbank account. The new provision is necessary to reconcile the law regarding the forfeiture of funds in bank accounts with the realities of the global movement of electronic funds and the use of off-shore banks to insulate criminal proceeds from forfeiture. “To prevent drug dealers and other criminals from taking advantage of certain nuances of forfeiture law to insulate their property from forfeiture even though it is deposited in a bank account in the United States, it is necessary to change the law regarding the location of the debt that a bank owes to its depositor, and the identity of the real party in interest with standing to contest the forfeiture. The amendment in this section addresses the location issue by treating a deposit made into an account in a foreign bank that has a correspondent account at a U.S. bank as if the deposit had been made into the U.S. bank directly. Second, the section treats the deposit in the correspondent account as a debt owed directly to the depositor, and not as a debt owed to the respondent bank. In other words, the correspondent account is treated as if it were the foreign bank itself, and the funds in the correspondent account were debts owed to the foreign bank's customers.

“Under this arrangement, if funds traceable to criminal activity are deposited into a foreign bank, the Government may bring a forfeiture action against funds in that bank's correspondent account, and only the initial depositor, and not the intermediary bank, would have standing to contest it.

“The section authorizes the Attorney General to suspend or terminate a forfeiture in cases where there exists a conflict of laws between the U.S. and the jurisdiction in which the foreign bank is located, where such suspension or termination would be in the interest of justice and not harm U.S. national interests”).

defendant may be ordered to transfer property to this country from overseas if the property is subject to confiscation.⁹⁹

Prior to enactment of the Act, federal law permitted confiscation of any property in the United States that could be traced to a drug offense committed overseas, if the offense was punishable as a felony under the laws of the nation where it occurred and if the offense would have been a felony if committed here.¹⁰⁰ Section 320 enlarges this provisions to cover not only drug offenses but any of the crimes in the money laundering predicate offense list of 18 U.S.C. 1956(c)(7)(B), and continues the reciprocal felony requirements.¹⁰¹ This treatment is comparable to the early coverage of the federal statute, 28 U.S.C. 2467, which permitted enforcement of foreign confiscation orders in the case of drug offenses or the crimes on the money laundering predicate offense list. Section 323 of the Act amends the foreign forfeiture enforcement statute to (1) expand the grounds for enforcement to include any crime which would have provided the grounds for confiscation had the offense been committed in the United States; (2) to authorize restraining orders to freeze the target property while enforcement litigation is pending; and (3) to limit the absence-of-timely-notice defense.¹⁰²

⁹⁹ Cf., H.R.Rep.No. 107-250, at 58-9 (2001) (“Section 116 authorizes a court to order a criminal defendant to repatriate his property to the United States in criminal cases. In criminal forfeiture cases, the sentencing court is authorized to order the forfeiture of ‘substitute assets’ when the defendant has placed the property otherwise subject to forfeiture ‘beyond the jurisdiction of the court.’ Frequently, this provision is applied when a defendant has transferred drug proceeds or other criminally derived property to a foreign country. In many cases, however, the defendant has no other assets in the United States of a value commensurate with the forfeitable property overseas. In such cases, ordering the forfeiture of substitute assets is a hollow sanction.

“This section amends 21 U.S.C. 853 to make clear that a court in a criminal case may issue a repatriation order—either post-trial as part of the criminal sentence and judgment, or pre-trial pursuant to the court’s authority under 21 U.S.C. 853(e) to restrain property—so that they will be available for forfeiture. Failure to comply with such an order would be punishable as a contempt of court, or it could result in a sentencing enhancement, such as a longer prison term, under the U.S. Sentencing Guidelines, or both”).

¹⁰⁰ 18 U.S.C. 981(a)(1)(B).

¹⁰¹ H.R.Rep.No. 107-250, at 56 (2001) (“This section is intended to reinforce the United States’ compliance with the Vienna Convention. It amends 18 U.S.C. 981(a)(1)(B) to allow the United States to institute its own action against the proceeds of foreign criminal offenses when such proceeds are found in the United States. As required by the Vienna Convention, it also authorizes the confiscation of property used to facilitate such crimes. The list of foreign crimes to which this section applies is determined by cross-reference to the foreign crimes that are money laundering predicates under 1956(c)(7)(B). This section will permit the forfeiture of property involved in conduct occurring before the effective date of the Act”).

¹⁰² H.R.Rep.No. 107-250, at 59-60 (2001) (“Under current law, 28 U.S.C. 2467(d) gives Federal courts the authority to enforce civil and criminal forfeiture judgments entered by foreign courts. This section amends that provision to include a mechanism for preserving property subject to forfeiture in a foreign country.

“Specifically, a Federal court could issue a restraining order under 18 U.S.C. 983(j) or register and enforce a foreign restraining order, if the Attorney General certified that such foreign order was obtained in accordance with the principles of due process. A person seeking

A fugitive may not challenge a federal forfeiture.¹⁰³ Section 322 applies this fugitive disentitlement to corporations whose major shareholder is a fugitive or whose representative in the confiscation proceedings is a fugitive.

Section 906 instructs the Attorney General, the Secretary of the Treasury, and the Director of Central Intelligence to submit a joint report with recommendations relating to the reconfiguration of the Foreign Terrorist Asset Tracking Center, the Office of Foreign Assets Control, and possibly FinCEN in “order to establish a capability to provide for the effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations.”

to contest the restraining order could do so on the ground that 28 U.S.C. 2467 was not properly applied to the particular case, but could not oppose the restraining order on any ground that could also be raised in the proceedings pending in a foreign court. This provision prevents a litigant from taking ‘two bites at the apple’ by raising objections to the basis for the forfeiture in the Federal court that he also raised, or is entitled to raise, in the foreign court where the forfeiture action is pending. It complements the existing provision in section 2467(e) providing that the Federal court is bound by the findings of fact of the foreign court, and may not look behind such findings in determining whether to enter an order enforcing a foreign forfeiture judgment.

“This section also amends 28 U.S.C. 2467 to make clear that it is not necessary to prove that the person asserting an interest in the property received actual notice of the forfeiture proceedings. As is the case with respect to forfeitures under U.S. law, it is sufficient if the foreign nation takes steps to provide notice, in accordance with the principles of due process. See *Gonzalez v. United States*, 1997 WL 278123 (S.D.N.Y. 1997) (‘the [G]overnment is not required to ensure actual receipt of notice that is properly mailed’); *Albajon v. Gugliotta*, 72 F. Supp. 2d 1362 (S.D. Fla. 1999) (notice sent to various addresses on claimant's identifications, and mailed after claimant released from jail, is sufficient to satisfy due process, even if claimant never received notice); *United States v. Schiavo*, 897 F. Supp. 644, 648 49 (D. Mass. 1995) (sending notice to fugitive's last known address is sufficient; due process satisfied even if he did not receive the notice).

“Finally, 28 U.S.C. 2467 is amended to authorize the enforcement of a forfeiture judgment based on any foreign offense that would constitute an offense giving rise to a civil or criminal forfeiture of the same property if the offense had been committed in the United States. This is one of two safeguards that the statute contains against the enforcement of judgments that the United States does not consider appropriate for enforcement: if the judgment is based on an act that would not constitute a crime in the United States, such as removing assets from the reach of a repressive regime, it could not be enforced. In addition, section 2467 already provides that a foreign judgment may only be enforced by a Federal court at the request of the United States, and only after the Attorney General has certified that the judgment was obtained in accordance with the principles of due process. Thus, neither a foreign Government nor a foreign private party could enforce a foreign judgment on its own under this provision.”). Note that the safeguard to which the report refers is the range of foreign offenses that will support an enforceable confiscation order, *i.e.*, drug offenses and crimes on the money laundering predicate offense list, and that the amendment narrows that safeguard by adding additional foreign offenses, *i.e.*, any foreign equivalent of a federal crime which would support a confiscation order.

¹⁰³ 28 U.S.C. 2466.

Alien Terrorists and Victims

The Act contains a number of provisions designed to prevent alien terrorists from entering the United States, particularly from Canada; to enable authorities to detain and deport alien terrorists and those who support them; and to provide humanitarian immigration relief for foreign victims of the attacks on September 11.

Border Protection. The border protection provisions:

- authorize the appropriations necessary to triple the number of Border Patrol, Customs Service, and Immigration and Naturalization Service (INS) personnel stationed along the Northern Border, section 401
- authorize appropriations of an additional \$50 million for both INS and the Customs Service to upgrade their border surveillance equipment, section 402
- remove for fiscal year 2001 the \$30,000 ceiling on INS overtime pay for border duty, section 404
- authorize appropriations of \$2 million for a report to be prepared by the Attorney General on the feasibility of enhancing the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and similar systems to improve the reliability of visa applicant screening, section 405
- authorize the appropriations necessary to provide the State Department and INS with criminal record identification information relating to visa applicants and other applicants for admission to the United States, section 403.
- instruct the Attorney General to report on the feasibility of the use of a biometric identifier scanning system with access to IAFIS for overseas consular posts and points of entry into the United States, section 1007
- direct the Secretary of State to determine whether consular shopping is a problem, to take any necessary corrective action, and to report the action taken, section 418
- express the sense of the Congress that the Administration should implement the integrated entry and exit data system called for by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1365a), section 414
- add the White House Office of Homeland Security to the Integrated Entry and Exit Data System Task Force (8 U.S.C. 1365a note), section 415
- call for the implementation and expansion of the foreign student visa monitoring program (8 U.S.C. 1372), section 416
- limit countries eligible to participate in the visa waiver program to those with machine-readable passports as of October 1, 2003 (8 U.S.C. 1187(c)), section 417

- instruct the Attorney General to report on the feasibility of using biometric scanners to help prevent terrorists and other foreign criminals from entering the country, section 1008¹⁰⁴
- authorize appropriations of \$250,000 for the FBI to determine the feasibility of providing airlines with computer access to the names of suspected terrorists, section 1009
- authorize reciprocal sharing of the State Department's visa lookout data and related information with other nations in order to prevent terrorism, drug trafficking, slave marketing, and gun running, section 413

Detention and Removal. Foreign nationals (aliens) are deportable from the United States, among other grounds, if they were inadmissible at the time they entered the country or if they have subsequently engaged in terrorist activity, 8 U.S.C. 1227 (a)(1)(A), (a)(4)(B), 1182(a)(3)(B)(iv). Aliens may be inadmissible for any number of terrorism-related reasons, 8 U.S.C. 1182 (a)(3)(B). Section 411 of the Act adds to the terrorism-related grounds upon which an alien may be denied admission into the United States and consequently upon which he or she may be deported.

Prior law recognized five terrorism-related categories of inadmissibility. Section 411 redefines two of these – engaging in terrorist activity and representing a terrorist organization (8 U.S.C. 1182(a)(3)(B)(iv), (a)(3)(B)(i)(IV)) – and it adds three more – espousing terrorist activity, being the spouse or child of an inadmissible alien associated with a terrorist organization, and intending to engage in activities that could endanger the welfare, safety or security of the United States (8 U.S.C. 1182(a)(3)(B)(i)(VI), (a)(3)(B)(i)(VII), 1182(a)(3)(F). It defined engaging in terrorist activity, which is grounds for both inadmissibility and deportation, to encompass soliciting on behalf of a terrorist organization or providing material support to a terrorist organization, 8 U.S.C. 1182(a)(3)(B)(iii)(2000 ed.). It did not explain in so many words, however, what constituted a “terrorist organization,” but it presumably included groups designated as terrorist organizations under section 219 of the Immigration and Nationality Act, 8 U.S.C. 1189.

Section 411 defines “terrorist organization” to include not only organizations designated under section 219 but also organizations which the Secretary of State has identified in the *Federal Register* as having provided material support for, committed, incited, planned, or gathered information on potential targets of, terrorist acts of violence, 8 U.S.C. 1182(a)(3)(B)(vi), (a)(3)(B)(iv). It then recasts the definition of engaging in terrorist activities to include solicitation on behalf of such organizations, or recruiting on their behalf, or providing them with material support, 8 U.S.C.

¹⁰⁴ As the House Judiciary Committee explained, “A biometric fingerprint scanning system is a sophisticated computer scanning technology that analyzes a person’s fingerprint and compares the measurement with a verified sample digitally stored in the system. The accuracy of these systems is claimed to be above 99.9%. The biometric identifier system contemplated by this section would have access to the database of the Federal Bureau of Investigation Integrated Automated Fingerprint Identification System,” H.R.Rep.No. 107-236, at 78 (2001).

1182(a)(3)(B)(iv). Nevertheless, section 411 permits the Secretary of State or Attorney General to conclude that the material support prohibition does not apply to particular aliens, 8 U.S.C. 1182(a)(3)(B)(vi).

Prior law made representatives of terrorist organizations designated by the Secretary under section 219 (8 U.S.C. 1189) inadmissible, 8 U.S.C. 1182(a)(3)(B)(i)(IV)(2000 ed.). And so they remain. Section 411 makes representatives of political, social or similar groups, whose public endorsements of terrorist activities undermines U.S. efforts to reduce or eliminate terrorism, inadmissible as well, 8 U.S.C. 1182(a)(3)(B)(i)(IV).

An individual who uses his or her place of prominence to endorse, espouse, or advocate support for terrorist activities or terrorist organizations in a manner which the Secretary of State concludes undermines our efforts to reduce or eliminate terrorism becomes inadmissible under section 411, 8 U.S.C. 1182(a)(3)(B)(i)(VI).

The spouse or child of an alien, who is inadmissible on terrorist grounds for activity occurring within the last 5 years, is likewise inadmissible, unless the child or spouse was reasonably unaware of the disqualifying conduct or has repudiated the disqualifying conduct, 8 U.S.C. 1182(a)(3)(B)(i)(VII), 1182(a)(3)(B)(ii).

Finally, any alien, whom the Secretary of State or the Attorney General conclude has associated with a terrorist organization and intends to engage in conduct dangerous to the welfare, safety, security of the United States while in this country, is inadmissible, 8 U.S.C. 1182(a)(3)(F).

Section 219 of the Immigration and Nationality Act (8 U.S.C. 1189) permits the Secretary to designate as terrorist organizations any foreign group which he finds to have engaged in terrorist activities. A second subsection 411(c) permits him to designate groups which as subnational groups or clandestine agents, engage in "premeditated, politically motivated violence perpetrated against noncombatant targets," or groups which retain the capacity and intent to engage in terrorism or terrorist activity, 8 U.S.C. 1189(a)(1)(B).

Section 412 permits the Attorney General to detain alien terrorist suspects for up to seven days, 8 U.S.C. 1226a. He must certify that he has reasonable grounds to believe that the suspects either are engaged in conduct which threatens the national security of the United States or are inadmissible or deportable on grounds of terrorism, espionage, sabotage, or sedition. Within seven days, the Attorney General must initiate removal or criminal proceedings or release the alien. If the alien is held, the determination must be reexamined every six months to confirm that the alien's release would threaten national security or endanger some individual or the general public. The Attorney General's determinations are subject to review only under writs of habeas corpus issued out of any federal district court but appealable only to the United States Court of Appeals for the District Columbia. The Attorney General must report to the Judiciary Committee on the details of the operation of section 412.

Uncertain is the relationship between section 412 and the President's Military Order of November 13, 2001, which allows the Secretary of Defense to detain designated alien terrorist suspects, within the United States or elsewhere, without

express limitation or condition except with regard to food, water, shelter, clothing, medical treatment, religious exercise, and a proscription on invidious discrimination, 66 *Fed.Reg.* 57833, 57834 (Nov. 16, 2001).

Victims. The Act contains a number of provisions designed to provide immigration relief for foreign nationals, victimized by the attacks of September 11. It provides for:

- permanent resident alien status for eligible aliens and members of their family who but for the events of September 11 would have been eligible for employer-sponsored permanent resident alien status, section 421¹⁰⁵
- extended filing deadlines for aliens prevented from taking timely action because of immigration office closures, airline schedule disruptions or other similar impediments, section 422¹⁰⁶

¹⁰⁵ “The Act provides permanent resident status through the special immigrant program to an alien who was the beneficiary of a petition filed (on or before September 11) to grant the alien permanent residence as an employer-sponsored immigrant or of an application for labor certification (filed on or before September 11), if the petition or application was rendered null because of the disability of the beneficiary or loss of employment of the beneficiary due to physical damage to, or destruction of, the business of the petitioner or applicant as a direct result of the terrorist attacks on September 11, or because of the death of the petitioner or applicant as a direct result of the terrorist attacks. Permanent residence would be granted to an alien who was the spouse or child of an alien who was the beneficiary of a petition filed on or before September 11 to grant the beneficiary permanent residence as a family-sponsored immigrant (as long as the spouse or child follows to join not later than September 11, 2003). Permanent residence would be granted to the beneficiary of a petition for a nonimmigrant visa as the spouse or the fiancé (and their children) of a U.S. citizen where the petitioning citizen died as a direct result of the terrorist attack. The section also provides permanent resident status to the grandparents of a child both of whose parents died as a result of the terrorist attacks, if either of such deceased parents was a citizen of the U.S. or a permanent resident,” H.R.Rep.No. 107-236, at 66-7 (2001).

¹⁰⁶ “The Act provides that an alien who was legally in a nonimmigrant status and was disabled as a direct result of the terrorist attacks on September 11 (and his or her spouse and children) may remain lawfully in the U.S. (and receive work authorization) until the later of the date that his or her status normally terminates or September 11, 2002. Such status is also provided to the nonimmigrant spouse and children of an alien who died as a direct result of the terrorist attacks.

“The Act provides that an alien who was lawfully present as a nonimmigrant at the time of the terrorist attacks will be granted 60 additional days to file an application for extension or change of status if the alien was prevented from so filing as a direct result of the terrorist attacks. Also, an alien who was lawfully present as a nonimmigrant at the time of the attacks but was then unable to timely depart the U.S. as a direct result of the attacks will be considered to have departed legally if doing so before November 11. An alien who was in lawful nonimmigrant status at the time of the attacks (and his or her spouse and children) but not in the U.S. at that time and was then prevented from returning to the U.S. in order to file a timely application for an extension of status as a direct result of the terrorist attacks will be given 60 additional days to file an application and will have his or her status extended 60 days beyond the original due date of the application.

“Under current law, winners of the fiscal year 2001 diversity visa lottery must enter the U.S. or adjust status by September 30, 2001. The Act provides that such an alien may enter

- preservation of certain immigration benefits available to alien family members that would be otherwise lost as a consequence of the death of a victim of September 11, section 423¹⁰⁷
- limited easing of age restrictions on visas available to aliens under 21 years of age for those whose 21st birthday occurred immediately before or soon after September 11, section 424¹⁰⁸
- temporary administrative relief for alien family members of a victim of September 11 who are not otherwise entitled to relief under the Act, section 425

the U.S. or adjust status until April 1, 2002, if the alien was prevented from doing so by September 30, 2001 as a direct result of the terrorist attacks. If the visa quota for the 2001 diversity visa program has already been exceeded, the alien shall be counted under the 2002 program. Also, if a winner of the 2001 lottery died as a direct result of the terrorist attacks, the spouse and children of the alien shall still be eligible for permanent residence under the program. The ceiling placed on the number of diversity immigrants shall not be exceeded in any case.

“Under the Act, in the case of an alien who was issued an immigrant visa that expires before December 31, 2001, if the alien was unable to timely enter the U.S. as a direct result of the terrorist attacks, the validity shall be extended until December 31.

“Under the Act, in the case of an alien who was granted parole that expired on or after September 11, if the alien was unable to enter the U.S. prior to the expiration date as a direct result of the terrorist attacks, the parole is extended an additional 90 days.

“Under the Act, in the case of an alien granted voluntary departure that expired between September 11 and October 11, 2001, voluntary departure is extended an additional 30 days,” H.R.Rep.No. 107-236, at 67-8 (2001).

¹⁰⁷ “Current law provides that an alien who was the spouse of a U.S. citizen for at least 2 years before the citizen died shall remain eligible for immigrant status as an immediate relative. This also applies to the children of the alien. The Act provides that if the citizen died as a direct result of the terrorist attacks, the 2 year requirement is waived.

“The Act provides that if an alien spouse, child, or unmarried adult son or daughter had been the beneficiary of an immigrant visa petition filed by a permanent resident who died as a direct result of the terrorist attacks, the alien will still be eligible for permanent residence. In addition, if an alien spouse, child, or unmarried adult son or daughter of a permanent resident who died as a direct result of the terrorist attacks was present in the U.S. on September 11 but had not yet been petitioned for permanent residence, the alien can self-petition for permanent residence.

“The Act provides that an alien spouse or child of an alien who 1) died as a direct result of the terrorist attacks and 2) was a permanent resident (petitioned-for by an employer) or an applicant for adjustment of status for an employment-based immigrant visa, may have his or her application for adjustment adjudicated despite the death (if the application was filed prior to the death),” H.R.Rep.No. 107-236, at 68 (2001)..

¹⁰⁸ “Under current law, certain visas are only available to an alien until the alien’s 21st birthday. The Act provides that an alien whose 21st birthday occurs this September and who is a beneficiary for a petition or application filed on or before September 11 shall be considered to remain a child for 90 days after the alien’s 21st birthday. For an alien whose 21st birthday occurs after this September, (and who had a petition for application filed on his or her behalf on or before September 11) the alien shall be considered to remain a child for 45 days after the alien’s 21st birthday,” H.R.Rep.No. 107-236, at 68 (2001).

- a denial of benefits of the Act to terrorists and their families, section 427
- authority for the Attorney General to establish evidentiary standards to implement the alien victim provisions of the Act, section 426.

Other Crimes, Penalties, & Procedures

New Crimes. The Act creates new federal crimes for terrorist attacks on mass transportation facilities, for biological weapons offenses, for harboring terrorists, for affording terrorists material support, for misconduct associated with money laundering already mentioned, for conducting the affairs of an enterprise which affects interstate or foreign commerce through patterned commission of terrorist offenses, and for fraudulent charitable solicitation. Although strictly speaking these are new federal crimes, they generally supplement existing law filling gaps and increasing penalties.

Pre-existing federal law criminalized, among other things, wrecking trains, 18 U.S.C. 1992, damaging commercial motor vehicles or their facilities, 18 U.S.C. 33, or threatening to do so, 18 U.S.C. 35, destroying vessels within the navigable waters of the United States, 18 U.S.C. 2273, destruction of vehicles or other property used in or used in activities affecting interstate or foreign commerce by fire or explosives, 18 U.S.C. 844(i), possession of a biological agent or toxin as a weapon or a threat, attempt, or conspiracy to do so, 18 U.S.C. 175, use of a weapon of mass destruction affecting interstate or foreign commerce or a threat, attempt, or conspiracy to do so, 18 U.S.C. 2332a, commission of a federal crime of violence while armed with a firearm, or of federal felony while in possession of an explosive, 18 U.S.C. 924(c), 844(h), conspiracy to commit a federal crime, 18 U.S.C. 371.

The Act outlaws terrorist attacks and other actions of violence against mass transportation systems. Offenders may be imprisoned for life or any term of years, if the conveyance is occupied at the time of the offense, or imprisoned for not more than twenty years in other cases, section 801. Under its provisions, it is a crime to willfully:

- wreck, derail, burn, or disable mass transit;
- place a biological agent or destructive device on mass transit recklessly or with the intent to endanger;
- burn or place a biological agent or destructive device in or near a mass transit facility knowing a conveyance is likely to be disabled;
- impair a mass transit signal system;
- interfere with a mass transit dispatcher, operator, or maintenance personnel in the performance of their duties recklessly or with the intent to endanger;
- act with the intent to kill or seriously injure someone on mass transit property;
- convey a false alarm concerning violations of the section;
- attempt to violate the section;
- threaten or conspire to violate the section

when the violation involves interstate travel, communication, or transportation of materials or that involves a carrier engaged in or affecting interstate or foreign commerce, 18 U.S.C. 1993.

Prior to enactment of the Act, federal law proscribed the use of biological agents or toxins as weapons, 18 U.S.C. 175. As suggested by the Justice Department,¹⁰⁹ the Act, in section 817, makes two substantial changes. It makes it a federal offense, punishable by imprisonment for not more than ten years and/or a fine of not more than \$250,000, to possess a type or quantity of biological material that cannot be justified for peaceful purposes, 18 U.S.C. 175(b). Second, consistent with federal prohibitions on the possession of firearms, 18 U.S.C. 922(g), and explosives, 18 U.S.C. 842(i), it makes it a federal offenses for certain individuals – such as convicted felons, illegal aliens, and fugitives – to possess biological toxins or agents, 18 U.S.C. 175b.¹¹⁰ Offenders face the same sanctions, imprisonment for not more than ten years and/or a fine of not more than \$250,000.

It is a federal crime to harbor aliens, 8 U.S.C. 1324, or those engaged in espionage, 18 U.S.C. 792; or to commit misprision of a felony (which may take the form of harboring the felon), 18 U.S.C. 4; or to act as an accessory after the fact to a federal crime (including by harboring the offender), 18 U.S.C. 3. The Justice Department had asked that a terrorist harboring offense be added to the espionage section. It also recommended venue and extraterritorial auxiliaries.¹¹¹

¹⁰⁹ “Current law prohibits the possession, development, acquisition, etc. of biological agents or toxins for use as a weapon. 18 U.S.C. §175. This section amends the definition of ‘for use as a weapon’ to include all situations in which it can be proven that the defendant had a purpose other than a prophylactic, protective, or peaceful purpose. This will enhance the government’s ability to prosecute suspected terrorists in possession of biological agents or toxins, and conform the scope of the criminal offense in 18 U.S.C. §175 more closely to the related forfeiture provision in 18 U.S.C. §176 [which permits confiscations in cases where the amounts possessed exceed the quantities justifiable for peaceful purposes]. Moreover, the section adds a subsection to 18 U.S.C. §175 which defines an additional offense of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective or other peaceful purpose. This section also enacts a new statute, 18 U.S.C. 175b, which generally makes it an offense for a person to possess a listed biological agent or toxin if the person is disqualified from firearms possession under 18 U.S.C. §922(g). . . .” *DoJ* at §305.

¹¹⁰ The section covers those under felony indictment, those convicted of a felony, fugitives, drug addicts, illegal aliens, mental defectives, aliens from countries which support terrorism, and those dishonorably discharged from the U.S. armed forces, 18 U.S.C. 175b(b)(2).

¹¹¹ “18 U.S.C. §792 makes it an offense to harbor or conceal persons engaged in espionage. There is no comparable provision for terrorism, though the harboring of terrorists creates a risk to the nation readily comparable to that posed by harboring spies. This section accordingly amends 18 U.S.C. §792 to make the same prohibition apply to harboring or concealing persons engaged in federal terrorism offenses as defined in section 309 of the bill,” *DoJ* at §307; *Draft* at §307(2) (“There is extraterritorial Federal jurisdiction over any violation (including, without limitation, conspiracy or attempt) of this section. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in Federal judicial district as provided by law”).

The Act, in section 803, instead establishes a separate offense which punishes harboring terrorists by imprisonment for not more than ten years and/or a fine of not more than \$250,000, 18 U.S.C. 2339. The predicate offense list consists of:

- destruction of aircraft or their facilities, 18 U.S.C. 32;
- biological weapons offenses, 18 U.S.C. 175;
- chemical weapons offenses, 18 U.S.C. 229;
- nuclear weapons offenses, 18 U.S.C. 831;
- bombing federal buildings, 18 U.S.C. 844(f);
- destruction of an energy facility, 18 U.S.C. 1366;
- violence committed against maritime navigational facilities, 18 U.S.C. 2280;
- offenses involving weapons of mass destruction, 18 U.S.C. 2232a;
- international terrorism, 18 U.S.C. 2232b;
- sabotage of a nuclear facility, 42 U.S.C. 2284;
- air piracy, 49 U.S.C. 46502.

It grants the Justice Department request to permit prosecution either in the place where the harboring occurred or where the underlying act of terrorism committed by the sheltered terrorist might be prosecuted. The Constitution, however, may insist that prosecution take place where the crime of harboring occurred.¹¹²

Sections 2339A and 2339B of the title 18 of the United States Code ban providing material support to individuals and to organizations that commit various crimes of terrorism. The Act amends the sections in several ways in section 805. Section 2339B (support of a terrorist organization) joins section 2339A (support of a terrorist) as a money laundering predicate offense, 18 U.S.C. 1956(c)(7)(D). The predicate offense list of 18 U.S.C. 2339A (support to terrorists) grows to include:

¹¹² *U.S. Const.* Art.III, §2, cl.3 (“The trial of all crimes . . . shall be held in the state where the said crimes shall have been committed”); Amend. IV (“In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed. . . .”); *United States v. Cabrales*, 524 U.S. 1 (1998)(a defendant charged with one count of conspiracy to launder the proceeds of a Missouri drug operation and two counts of laundering in Florida could not be prosecuted in Missouri on the laundering counts). The Court might be thought to have retreated somewhat from *Cabrales* when it later approved prosecution for carrying a firearm in relation to a crime of violence in federal court in New Jersey (where the underlying kidnaping occurred) notwithstanding the fact that the firearm had been acquired in Maryland after the defendants left New Jersey with their victim in tow, *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280-81 n.4 (1999)(“By way of comparison, last Term in [*Cabrales*] we considered whether venue for money laundering, in violation of 18 U.S.C. 1956(a)(1)(B) (ii) and 1957, was proper in Missouri, where the laundered proceeds were unlawfully generated, or rather, only in Florida, where the prohibited laundering transactions occurred. As we interpreted the laundering statutes at issue, they did not proscribe the anterior criminal conduct that yielded the funds allegedly laundered. The existence of criminally generated proceeds was a circumstance element of the offense but the proscribed conduct – defendant’s money laundering activity – occurred after the fact of an offense begun and completed by others. Here, by contrast, given the ‘during and in relation to’ language [of section 924], the underlying crime of violence is a critical part of the §924(c)(1) offense”).

- chemical weapons offenses, 18 U.S.C. 229;
- terrorist attacks on mass transportation, 18 U.S.C. 1993 ;
- sabotage of a nuclear facility, 42 U.S.C. 2284; and
- sabotage of interstate pipelines, 49 U.S.C. 60123(b).

And it adds expert advice or assistance to the types of assistance that may not be provided under section 2339A. This last addition may encounter the same First Amendment vagueness problems some courts have found in assistance which takes the form of “training” and “personnel,” *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 1137-136 (9th Cir. 2000).¹¹³ Finally, the section announces that a prosecution for violation of section 2339A (support of terrorists) may be brought where the support is provided or where the predicate act of terrorism occurs. There may be some question whether the Constitution permits prosecution where the predicate act occurs.¹¹⁴

Section 813 of the Act also accepts the Justice Department's suggestion that various terrorism offenses be added to the predicate offense list for RICO (racketeer influenced and corrupt organizations) which proscribes acquiring or operating, through the patterned commission of any of a series of predicate offenses, an enterprise whose activities affect interstate or foreign commerce, 18 U.S.C. 1961.¹¹⁵

Prior law, 18 U.S.C. 2325-2327, outlawed violation of Federal Trade Commission (FTC) telemarketing regulations promulgated under 15 U.S.C. 6101 *et seq.* Section 1011 of the Act brings fraudulent charitable solicitations within the FTC's regulatory authority.¹¹⁶

¹¹³ The Justice Department sought the expansion along with the enlargement of the predicate offense list, “18 U.S.C. §2339A prohibits providing material support or resources to terrorists. The existing definition of ‘material support or resources’ is generally not broad enough to encompass expert services and assistance – for example, advice provided by a person with expertise in aviation matters to facilitate an aircraft hijacking, or advice provided by an accountant to facilitate the concealment of funds used to support terrorist activities. This section accordingly amends 18 U.S.C. §2339A to include expert services and assistance, making the offense applicable to experts who provide services or assistance knowing or intending that the services or assistance is to be used in preparing for or carrying out terrorism crimes. This section also amends 18 U.S.C. §2339A to conform its coverage of terrorism crimes to the more complete list specified in section 309 of the bill (‘Federal terrorism offenses’),” *DoJ* at 306.

¹¹⁴ *U.S. Const.* Art.III, §2, cl.3; Amend. IV; *United States v. Cabrales*, 524 U.S. 1 (1998); *United States v. Rodriguez-Moreno*, 526 U.S. 275 (1999).

¹¹⁵ “The list of predicate federal offenses for RICO, appearing in 18 U.S.C. §1961(1), includes none of the offenses which are most likely to be committed by terrorists. This section adds terrorism crimes to the list of RICO predicates, so that RICO can be used more frequently in the prosecution of terrorist organizations. As in various other provisions, the list of offenses in section 309 of the bill (‘Federal terrorism offenses’) is used in identifying the relevant crimes,” *DoJ*, at §304.

¹¹⁶ For a general discussion, *see*, Wellborn, *Combating Charitable Fraud: An Overview of State and Federal Law*, CRS REP.NO. RS21058 (Nov. 7, 2001).

New Penalties. The Act increases the penalties for acts of terrorism and for crimes which terrorists might commit. More specifically it establishes an alternative maximum penalty for acts of terrorism, raises the penalties for conspiracy to commit certain terrorist offenses, envisions sentencing some terrorists to life-long parole, and increases the penalties for counterfeiting, cybercrime, and charity fraud.

The Justice Department suggested an alternative term of imprisonment up to life imprisonment for anyone convicted of an offense designated a terrorist crime. It characterized its proposal as analogous to the standard fine provisions of 18 U.S.C. 3571(b),(c). Section 3571 sets a basic maximum fine of \$250,000 for any individual who convicted of a federal felony notwithstanding any lower maximum fine called for in the statute that outlaws the offense.¹¹⁷

The proposal, however, failed to identify the critical elements that would trigger the alternative.¹¹⁸ Both practical and constitutional challenges might be thought to attend this failure to distinguish between those convicted of some “garden variety” crime of terrorism and the more serious offender meriting the alternative, supplementary penalty. Perhaps for this reason, the Act opted to simply increase the maximum penalties for various crimes of terrorism, particularly those which involve the taking of a human life and are not already capital offenses, section 810. Thus, it increases the maximum terms imprisonment for:

- for life-threatening arson or arson of a dwelling committed within a federal enclave, from 20 years to any term of years or life, 18 U.S.C. 81;
- for causing more than \$100,000 in damage to, or significantly impairing the operation of an energy facility, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 1366;

¹¹⁷ “Under existing law, the maximum prison terms for federal offenses are normally determined by specifications in the provisions which define them. These provisions can provide inadequate maxima in cases where the offense is aggravated by its terrorist character or motivation. This section accordingly adds a new subsection (e) to 18 U.S.C. §3559 which provides alternative maximum prison terms, including imprisonment for any term of years or for life, for crimes likely to be committed by terrorists. This is analogous to the maximum fine provisions of 18 U.S.C. §3571(b)-(c) – which supersede lower fine amounts specified in the statutes defining particular offenses – and will more consistently ensure the availability of sufficiently high maximum penalties in terrorism cases. As in several other provisions of this bill, the list of the serious crimes most frequently committed by terrorists set forth in section 309 of the bill (‘Federal terrorism offenses’ is used in defining the scope of the provision,” *DoJ*, at §302.

¹¹⁸ “A person convicted of any Federal terrorism offense may be sentenced to imprisonment for any term of years or for life, notwithstanding any maximum term of imprisonment specified in the law describing the offense. The authorization of imprisonment under this subsection is supplementary to, and does not limit, the availability of any other penalty authorized by the law describing the offense, including the death penalty, and does not limit the applicability of any mandatory minimum term of imprisonment, including any mandatory life term, provided by the law describing the offense,” *Draft* at §302.

- for providing material support to a terrorist or a terrorist organization, from 10 to 15 years (or any term of years or life, if death results), 18 U.S.C. 2339A, 2339B;
- for destruction of national defense materials, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 2155;
- for sabotage of a nuclear facility, from 10 to 20 years (or any term of years or life, if death results), 42 U.S.C. 2284;
- for carrying a weapon or explosive aboard an aircraft with U.S. special aircraft jurisdiction, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 46505; and
- for sabotage of interstate gas pipeline facilities, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 60123.

It is a separate federal offense punishable by imprisonment for not more than five years to conspire to commit any federal felony, 18 U.S.C. 371. Co-conspirators are likewise subject to punishment for the underlying offense and for any other crimes committed in furtherance of the conspiracy. Nevertheless, some federal criminal statutes impose the same penalties for both the crimes they proscribe and any conspiracy to commit them. The Justice Department urged similar treatment for crimes of terrorism.¹¹⁹ Again, the Act, in section 811, opts for a less sweeping approach and establishes equivalent sanctions for conspiracy and the underlying offense in cases of:

- arson committed within a federal enclave, 18 U.S.C. 81;
- killing committed while armed with a firearm in a federal building, 18 U.S.C. 930(c);
- destruction of communications facilities, 18 U.S.C. 1362;
- destruction of property within a federal enclave, 18 U.S.C. 1363;
- causing a train wreck, 18 U.S.C. 1922;
- providing material support to a terrorist, 18 U.S.C. 2339A;
- torture committed overseas under color of law, 18 U.S.C. 2340A;
- sabotage of a nuclear facility, 42 U.S.C. 2284;

¹¹⁹ “The maximum penalty under the general conspiracy provision of federal criminal law (18 U.S.C. §371) is five years, even if the object of the conspiracy is a serious crime carrying a far higher maximum penalty. For some individual offenses and types of offense, special provisions authorize conspiracy penalties equal to the penalties for the object offense – see e.g., 21 U.S.C. §846 (drug crimes) – but there is no consistently applicable provision of this type for the crimes that are likely to be committed by terrorists.

“This section accordingly adds a new §2332c to the terrorism chapter of the criminal code – parallel to the drug crime conspiracy provision in 21 U.S.C. §846 – which provides maximum penalties for conspiracies to commit terrorism crimes that are equal to the maximum penalties authorized for the objects of such conspiracies. This will more consistently provide adequate penalties for terrorist conspiracies. As in various other provisions of this bill, the relevant class of offenses is specified by the notion of ‘Federal terrorism offense,’ which is defined in section 309 of the bill,” *DoJ* at §303.

- interfering with a flight crew within U.S. special aircraft jurisdiction, 49 U.S.C. 46504;
- carrying a weapon or explosive aboard an aircraft within U.S. special aircraft jurisdiction, 49 U.S.C. 46505; and
- sabotage of interstate gas pipeline facilities, 49 U.S.C. 60123.

When federal courts impose a sentence of a year or more upon a convicted defendant, they must also impose a term of supervised release, 18 U.S.C. 3583; U.S.S.G. §5D1.1. Supervised release is not unlike parole, except that it is ordinarily imposed in addition to (rather than in lieu of) a term, or portion of a term, of imprisonment. The term may be no longer than 5 years for most crimes and violations of the conditions of release may result in imprisonment for up to an additional 5 years, 18 U.S.C. 3583(e). The terms of supervisory release for drug dealers, however, are often cast as mandatory minimums with no statutory ceiling. Thus, for example, a dealer convicted of distributing more than a kilogram of heroin must receive a term of supervised release of “at least 5 years” in addition to a term of imprisonment imposed for the offense, 21 U.S.C. 841(b). Although a majority feel that the more specific drug provisions of 21 U.S.C. 841 trump the more general limitations of 18 U.S.C. 3583, some of the federal appellate courts believe the two should be read in concert where possible (*e.g.*, at least but not more than 5 years).¹²⁰ The Justice Department recommended a maximum supervisory term of life for those convicted of acts of terrorism (subject to the calibrations of the Sentencing Commission),¹²¹ a recommendation which the Act accepted in section 812 but only in the case of terrorists whose crimes resulted in death or were marked by a foreseeable risk of death or serious bodily injury, 18 U.S.C. 3583(j).

¹²⁰ Compare, *United States v. Barragan*, 263 F.3d 919, 925-26 (9th Cir. 2001); *United States v. Pratt*, 239 F.3d 640, 646-48 (4th Cir. 2001); *United States v. Heckard*, 238 F.3d 1222, 1237 (10th Cir. 2001); and *United States v. Aguayo-Delgado*, 220 F.3d 926, 933 (8th Cir. 2000); with, *United States v. Meshack*, 225 F.3d 556, 578 (5th Cir. 2001); and *United States v. Samour*, 199 F.3d 821, 824-25 (6th Cir. 2001).

¹²¹ “Existing federal law (18 U.S.C. 3583(b)) generally caps the maximum period of post-imprisonment supervision for released felons at 3 or 5 years. Thus, in relation to a released but still unreformed terrorist, there is no means of tracking the person or imposing conditions to prevent renewed involvement in terrorist activities beyond a period of a few years. The drug laws (21 U.S.C. §841) mandate longer supervision periods for persons convicted of certain drug trafficking crimes, and specify no upper limit on the duration of supervision, but there is nothing comparable for terrorism offenses.

“This section accordingly adds a new subsection to 18 U.S.C. 3583 to authorize longer supervision periods, including potentially lifetime supervision, for persons convicted of terrorism crimes. This would permit appropriate tracking and oversight following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments. As in other provisions in this bill, the covered class of crimes is federal terrorism offenses, which are specified in section 390 of the bill.

“This section affects only the maximum periods of post-release supervision allowed by statute. It does not limit the authority of the Sentencing Commission and the courts to tailor the supervision periods imposed in particular cases to offense and offender characteristics, and the courts will retain their normal authority under 18 U.S.C. §3583(e)(1) to terminate supervision if it is no longer warranted,” *DoJ* at §308.

Sometime ago, Congress outlawed computer fraud and abuse (cybercrime) involving “federal protected computers” (*i.e.*, those owned or used by the federal government or by a financial institution or used in interstate or foreign commerce), 18 U.S.C. 1030. Section 814 of the Act increases the penalty for intentionally damaging a protected computer from imprisonment for not more than 5 years to imprisonment for not more than 10 years (from not more than 10 to not more than 20 years for repeat offenders).¹²²

Finally, section 1011 increases the penalty for fraudulently impersonating a Red Cross member or agent (18 U.S.C. 917) from imprisonment for not more than 1 year to imprisonment for not more than 5 years.

Other Procedural Adjustments. In other procedural adjustments designed to facilitate criminal investigations, the Act:

- increases the rewards for information in terrorism cases
- expands the Posse Comitatus Act exceptions
- authorizes “sneak and peek” search warrants
- permits nationwide and perhaps worldwide execution of warrants in terrorism cases
- eases government access to confidential information
- allows the Attorney General to collect DNA samples from prisoners convicted of any crime of violence or terrorism
- lengthens the statute of limitations applicable to crimes of terrorism
- clarifies the application of federal criminal law on American installations and in residences of U.S. government personnel overseas
- adjusts federal victims’ compensation and assistance programs

A section found in the Senate bill, but ultimately dropped, would have changed the provision of law that required Justice Department prosecutors to adhere to the ethical standards of the legal profession where they conduct their activities (the McDade-Murtha Amendment), 28 U.S.C. 530B.¹²³

¹²² It provides a comparable increase to not more than 20 years (from not more than 10 years) for those who recklessly damage a protected computer following a prior computer abuse conviction. Civil and criminal liability for simply causing protected computer damage (as opposed to intentionally or reckless causing the damage) is limited to special circumstances, *e.g.*, damage in excess of \$5000, damage causing physical injury, etc.; section 814 adds to the list of circumstances upon which liability may be predicated. To the list of predicate circumstances, it adds causing damage to a computer used by the government for the administration of justice, national defense, or national security.

¹²³ When presenting the final bill to the House, the Chairman of the Judiciary Committee noted, “the Senate bill contained revisions of the so-called McDade law. This compromise version does not contain those changes, and I agreed to review this subject in a different context,” 147 *Cong. Rec.* H7196 (daily ed. Oct. 23, 2001)(remarks of Rep. Sensenbrenner); for general background, *see*, Doyle, *McDade-Murtha Amendment: Ethical Standards for Justice Department Attorneys*, CRS REP.NO. RL30060 (Dec. 14, 2001).

Rewards. The Attorney General already enjoys the power to pay rewards in criminal cases, but his powers under other authorities is often subject to caps on the amount he might pay. Thus as a general rule, he may award amounts up to \$25,000 for the capture of federal offenders, 18 U.S.C. 3059, and may pay rewards in any amount in recognition of assistance to the Department of Justice as long as the Appropriations and Judiciary Committees are notified of any rewards in excess of \$100,000, 18 U.S.C. 3059B. Although he has special reward authority in terrorism cases, individual awards were capped at \$500,000, the ceiling for the total amount paid in such rewards was \$5 million, and rewards of \$100,000 or more required his personal approval or that of the President, 18 U.S.C. 3071-3077. Over the last several years, annual appropriation acts have raised the \$500,000 cap to \$2 million and the \$5 million ceiling to \$10 million, *e.g.*, P.L. 106-553, 114 Stat. 2762-67 (2000); P.L. 106-113, 113 Stat. 1501A-19 (1999); P.L. 105-277, 112 Stat. 2681-66 (1998).

The Act supplies the Attorney General with the power to pay rewards to combat terrorism in any amount and without an aggregate limitation, but for rewards of \$250,000 or more it insists on personal approval of the Attorney General or the President and on notification of the Appropriations and Judiciary Committees, section 501 (18 U.S.C. 3071). In addition, the counterterrorism fund of section 101 can be used "without limitation" to pay rewards to prevent, investigate, or prosecute terrorism.¹²⁴

The Secretary of State's reward authority was already somewhat more generous than that of the Attorney General. He may pay rewards of up to \$5 million for information in international terrorism cases as long as he personally approves payments in excess \$100,000, 22 U.S.C. 2708. The Act removes the \$5 million cap and allows rewards to be paid for information concerning the whereabouts of terrorist leaders and facilitating the dissolution of terrorist organizations, section 502.

Posse Comitatus. The Posse Comitatus Act and its administrative auxiliaries, 18 U.S.C. 1385, 10 U.S.C. 375, ban use of the armed forces to execute civilian law, absent explicit statutory permission. One existing statutory exception covers Department of Justice requests for technical assistance in connection with emergencies involving biological, chemical or nuclear weapons, 18 U.S.C. 2332e, 10 U.S.C. 382. The Act enlarges the exception to include emergencies involving other weapons of mass destruction, section 104.¹²⁵

Delayed notification of a search (sneak and peek). Rule 41 of the Federal Rules of Criminal Procedure seemed to preclude "sneak and peek" warrants before passage of the Act. A sneak and peek warrant is one that authorizes officers to secretly enter, either physically or virtually; conduct a search, observe, take

¹²⁴ The fund is otherwise available to reestablish capacity lost in terrorist attacks, to conduct threat assessments for federal agencies, and to reimburse federal agencies for the costs of detaining terrorist suspects overseas.

¹²⁵ For a general discussion of the Posse Comitatus Act, *see*, Doyle, *The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law*, CRS REP.NO. 95-964 (June 1, 2000).

measurements, conduct examinations, smell, take pictures, copy documents, download or transmit computer files, and the like; and depart without taking any tangible evidence or leaving notice of their presence. The Rule required that after the execution of a federal search warrant officers leave a copy of the warrant and an inventory of what they have seized (tangible or intangible), and they were to advise the issuing court what they had done, F.R.Crim.P. 41(d). To what extent did Rule 41 portray the standards for a reasonable search and seizure for purposes of the Fourth Amendment?

The Fourth Amendment clearly requires officers to knock and announce their purpose before entering to execute a warrant, *Richards v. Wisconsin*, 520 U.S. 385 (1997), but with equal clarity recognizes exceptions for exigent circumstances such as where compliance will lead to the destruction of evidence, flight of a suspect, or endanger the officers, *Wilson v. Arkansas*, 514 U.S. 927 (1995). It is undisputed that Title III (the federal wiretap statute) is not constitutionally invalid because it permits delayed notice of the installation of an interception device, *Dalia v. United States*, 441 U.S. 238 (1979). Finally, there is no doubt that the Fourth Amendment imposes no demands where it does not apply. Thus, chapter 121 (court authorization for disclosure of the contents of e-mail stored with third party service providers) may permit delayed notification of the search of e-mail in remote storage with a third party for more than 180 days without offending the Fourth Amendment, because there is no Fourth Amendment justifiable expectation of privacy under such circumstances, *cf.*, *United States v. Miller*, 425 U.S. 435 (1976).

The lower federal courts are divided over the extent to which the Rule reflects Fourth Amendment requirements. The Ninth Circuit saw the Fourth Amendment reflected in Rule 41, *United States v. Freitas*, 800 F.2d 1451, 1453 (9th Cir. 1986).¹²⁶

¹²⁶ “The district court held that a search warrant permitting agents to observe, but not seize tangible property was impermissible under Rule 41. That holding conflicts with language in *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977): Although Rule 41(h) defines property to include documents, books, papers, and any other tangible objects, it does not restrict or purport to exhaustively enumerate all the items which may be seized pursuant to Rule 41. . . . Rule 41 is not limited to tangible items. That case held seizures of intangibles were not precluded by the definition of property appearing in Rule 41(b). Without doubt there was a search in this case. Its purpose, we hold, was to seize intangible, not tangible, property. The intangible property to be seized was information regarding the status of the suspected clandestine methamphetamine laboratory. The search was authorized by a warrant supported by what the district court concluded was probable cause. . . . The question remains, however, whether a warrant lacking both a description of the property to be seized and a notice requirement conforms to Rule 41. . . . we hold that there was no compliance with Rule 41 under the facts of this case. . . . While it is clear that the Fourth Amendment does not prohibit all surreptitious entries, it is also clear that the absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy. We resolve those doubts by holding that in this case the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing of necessity. We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interests, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth

The Second Circuit was less convinced and preferred to hold sneak and peek searches to the demands of Rule 41, *United States v. Pangburn*, 983 F.2d 449 (2d Cir. 1993).¹²⁷ The Fourth Circuit was, if anything, less convinced. Moreover, the facts in the case demonstrate the potential impact of the issue on computer privacy, *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).¹²⁸

Amendment, demands that surreptitious entries be closely circumscribed,” *United States v. Freitas (Freitas I)*, 800 F.2d 1451, 1455-456 (9th Cir. 1986). The court remanded the case for a determination of whether grounds existed for a good faith exception to application of the exclusionary rule. It subsequently declined to exclude the evidence on those grounds, *United States v. Freitas (Freitas II)*, 856 F.2d 1425 (9th Cir. 1988).

¹²⁷ “No provision specifically requiring notice of the execution of a search warrant is included in the Fourth Amendment. Accordingly, in *Dalia v. United States*, 441 U.S. 238, 247 (1979), the Supreme Court found no basis for a constitutional rule proscribing all covert entries. Resolving the particular issue raised in *Dalia*, the Court determined that the Fourth Amendment does not prohibit per se a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment. Rule 41 of the Federal Rules of Criminal Procedure does require notice of the execution of a search warrant but does not prescribe when the notice must be given. Rule 41 by its terms provides for notice only in the case of seizures of physical property. . . . The Supreme Court also has held that the authority conferred by Rule 41 is not limited to the seizure of tangible items. See *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977). Despite the absence of notice requirements in the Constitution and Rule 41, it stands to reason that notice of a surreptitious search must be given at some point after the covert entry. . . . Although the *Freitas I* court specifically determined that the warrant was constitutionally defective for failure to include a notice requirement, we made no such determination in *United States v. Villegas*, 899 F.2d 1324 (1999). Although the *Freitas I* court found that covert entry searches without physical seizure strike at the very heart of the Fourth Amendment-protected interests, we used no such language in *Villegas*. Indeed, it was our perception that a covert entry search for intangibles is less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. . . . We prefer to root out notice requirement in the provisions of Rule 41 rather than in the somewhat amorphous Fourth Amendment interests concept developed by the *Freitas I* court. The Fourth Amendment does not deal with notice of any kind, but Rule 41 does. It is from the Rule's requirements for service of a copy of the warrant and for provision of an inventory that we derive the requirements of notice in cases where a search warrant authorizes covert entry to search and to seize intangibles,” *United States v. Pangburn*, 983 F.2d 449, 453-55 (2d Cir. 1993).

¹²⁸ In *Simons*, a search team entered Simons' office at night in his absence and “copied the contents of Simons' computer; computer diskettes found in Simons' desk drawer; computer files stored on the zip drive or on zip drives diskettes; videotapes; and various documents, including personal correspondence. No original evidence was removed from the office. Neither a copy of the warrant nor a receipt for the property seized was left in the office or otherwise given to Simons at that time, and Simons did not learn of the search for approximately 45 days.” A property list, however, was returned to the magistrate. In the view of the Fourth Circuit, “[t]here are two categories of Rule 41 violations; those involving constitutional violations and all others. The violations termed ‘ministerial’ in our prior cases obviously fall into the latter category. Nonconstitutional violations of Rule 41 warrant suppression only when the defendant is prejudiced by the violation, or when there is evidence of intentional and deliberate disregard of a provision in the Rule. First, we conclude that the failure of the team executing the warrant to leave either a copy of the warrant or a receipt for the items taken did not render the search unreasonable under the Fourth Amendment. The

The Justice Department urged that the conflict be resolved with a uniform rule which permitted sneak and peek warrants under the same circumstances that excused delayed notification of government access to e-mail to longer-term, remote, third party storage.¹²⁹

The Act, in section 213, stops short of the Justice Department proposal. Characterized as a codification of the Second Circuit decision, 147 *Cong. Rec.* H7197 (daily ed. Oct. 23, 2001), the Act extends the delayed notification procedure of chapter 121, which operates in an area to which the Fourth Amendment is inapplicable, to cases to which the Fourth Amendment applies, 18 U.S.C. 3103a. Its sneak and peek authorization reaches all federal search and seizure warrants where the court finds reasonable cause to believe that notification would have the kind of adverse results depicted in 18 U.S.C. 2705. Section 2705 describes both exigent circumstances (*e.g.*, risk of destruction of evidence or bodily injury) and circumstances that are not likely to excuse notification when it is required by the Fourth Amendment (*e.g.*, jeopardizing an investigation; delaying a trial). The sneak and peek authorization, however, does not reach tangible evidence, or wire or electronic communication unless the court finds the seizure “reasonably necessary.” It is not clear whether reasonable necessity means a seizure necessary to the investigation that is also reasonable in a Fourth Amendment sense, *i.e.*, in the presence of exigent circumstances, or whether it means a seizure which a reasonable judge might find necessary for the investigation.¹³⁰ The doctrine of constitutional avoidance argues against the latter interpretation. By the same token, when the Act permits delay for a reasonable period, it should probably be understood to mean

Fourth Amendment does not mention notice, and the Supreme Court has stated that the constitution does not categorically proscribe covert entries, which necessarily involve a delay in notice. And insofar as the August search satisfied the requirements of the Fourth Amendment, *i.e.*, it was conducted pursuant to a warrant based on probable cause issued by a neutral and detached magistrate, we perceive no basis for concluding that the 45-day delay in notice rendered the search unconstitutional. Having concluded that the Rule 41(d) violation at issue here did not infringe on Simons' constitutional rights, we must now evaluate his argument that the violation was deliberate. . . . The district court did not address the intent issue when it ruled on Simons' motion to suppress. . . . We therefore remand for the district court to consider whether the Government intentionally and deliberately disregarded the notice provision of Rule 41(d) when it carried out the August 6, 1998 search,” 206 F.3d at 403.

¹²⁹ “The law that currently governs notice to subjects of warrants where there is a showing to the court that immediate notice would jeopardize an ongoing investigation or otherwise interfere with lawful law enforcement activities, is a mix of inconsistent rules, practices, and court decisions varying widely from jurisdiction to jurisdiction across the country. This greatly hinders the investigation of many terrorism cases and other cases. This section resolves this problem by establishing a statutory, uniform standard for all such circumstances. It incorporates by reference the familiar, court-enforced standards currently applicable to stored communications under 18 U.S.C. §2705, and applies them to all instances where the court is satisfied that immediate notice of execution of a search warrant would jeopardize an ongoing investigation or otherwise interfere with lawful law-enforcement activities,” *DoJ* at §353.

¹³⁰ Since neither the restriction nor its reasonable necessity exception appeared in the Justice Department's initial proposal, the Department's justification does not address the question.

constitutionally “reasonable,” that is, a brief period reasonable in light of the exigent circumstances which allow the delay or their like.

Nationwide terrorism search warrants. The Fourth Amendment demands that warrants be issued by a neutral magistrate, *Coolidge v. New Hampshire*, 403 U.S. 443 (1971); the Sixth Amendment, that crimes be prosecuted in the districts where they occur, *United States v. Cabrales*, 524 U.S. 1 (1998). The Federal Rules direct magistrates to issue warrants only for property within their judicial district, although they permit execution outside the district for property located in the district when the warrant is sought but removed before execution can be had, F.R.Crim.P. 41(a).

The Act, in section 219, allows a magistrate in the district in which a crime of terrorism has occurred to issue a search warrant to be executed either “within or outside the district,” (F.R.Crim.P. 41(a)(3)) in domestic and international terrorism cases.¹³¹ The provision may anticipate execution both in this country and overseas.¹³² The Fourth Amendment does not apply to the overseas searches of the property of foreign nationals, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). It does apply to the search of American property overseas involving American authorities, although the lower federal courts are divided over the exact level of participation required to trigger coverage.¹³³ Neither Rule 41 nor any other provision of federal

¹³¹ The amended rule uses the definitions of domestic and international terrorism found in 18 U.S.C. 2331, as modified by section 802 of the Act: “(1) the term ‘international terrorism’ means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . (5) the term ‘domestic terrorism’ means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States,” 18 U.S.C. 2331(1),(5).

¹³² The Justice Department, with whom the proposal originated, was somewhat cryptic on this point. Its analysis suggests execution in one of the several judicial districts of the United States, but not so precisely as to negate any other construction. “The restrictiveness of the existing rule creates unnecessary delays and burdens for the government in the investigation of terrorist activities and networks that span a number of districts, since warrants must be separately obtained in each district. This section resolves that problem by providing that warrants can be obtained in any district in which activities related to the terrorism may have occurred, regardless of where the warrants will be executed,” *DoJ* at §351.

¹³³ *United States v. Barona*, 56 F.3d 1087, 1092 (9th Cir. 1995)(“United States agents’ participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials”); *United States v. Behety*, 32 F.3d 503, 510 (11th Cir. 1994)(“if American law enforcement officials substantially participated in the search or if the

law apparently contemplated extraterritorial execution, *cf.*, F.R.Crim.P.41, *Advisory Committee Notes: 1990 Amendment* (discussing a proposal for extraterritorial execution that the Supreme Court rejected).¹³⁴

If the Act anticipates overseas execution there may be some question whether it creates a procedure to be used in lieu of extradition when the person for whom the search warrant has been issued is located outside the United States. The section refers to warrants for “search of property *or for a person* within or outside the district,” §219 (emphasis added). The Judicial Conference in 1990 recommended an amendment to Rule 41, which the Supreme Court rejected, that would have permitted the overseas execution of federal search warrants. In doing so, the Conference suggested extraterritorial execution be limited to warrants to search for property and not reach warrants to search for persons, “lest the rule be read as a substitute for extradition proceedings,” F.R.Crim.P. 41, *Advisory Committee Notes: 1990 Amendment*. There is no indication, however, that the section is at odds with either the Fourth or Sixth Amendment.

Terrorists’ DNA. The courts have generally concluded that the collection of DNA information from convicted prisoners does not offend constitutional standards *per se*.¹³⁵ Existing federal law allowed the Attorney General to collect samples from

foreign officials conducting the search were actually acting as agents for their American counterparts”); *United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992) (“where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials” or “where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials”); *United States v. Mitro*, 880 F.2d 1480, 1482 (1st Cir. 1989) (“where American agents participated in the foreign search or the foreign officers acted as agents for their American counterparts”); *United States v. Mount*, 757 F.2d 1315, 1318 (D.C.Cir. 1985) (“if American officials or officers participated in some significant way”); *United States v. Marzano*, 537 F.2d 257, 270 (7th Cir. 1976) (declining to adopt the “joint venture” standards, but finding level of American participation in the case before it insignificant); *United States v. Morrow*, 537 F.2d 120, 139 (5th Cir. 1976) (“if American law enforcement officials participated in the foreign search, or if the foreign authorities actually conducting the search were acting as agents for their American counterparts”); each of the decisions also suggests that evidence secured in a manner which shocked the conscience of the court would be excluded.

¹³⁴ The Code still carries remnants of the consular courts which speak of the overseas execution of arrest warrants in places where the United States has “extraterritorial jurisdiction,” 18 U.S.C. 3042. The history of the provisions makes it clear that the phrase “extraterritorial jurisdiction” was intended to coincide with those places in which the U.S. had consular courts, *see*, S.Rep. 217, 73d Cong., 2d Sess. 3 (1934), *reprinted*, 78 *Cong.Rec.* 4982-983 (1934) (“The countries to which the proposed bill, if enacted into law, would relate are the following, in which the United States exercises extraterritorial jurisdiction: China, Egypt, Ethiopia, Muscat, and Morocco”); 22 U.S.C. 141 (1926 ed.) (conferring judicial powers on consular courts there identified as those located in China, Egypt, Ethiopia, Muscat, Morocco, Siam and Turkey).

¹³⁵ *Roe v. Marcotte*, 193 F.3d 72 (2d Cir. 1999); *Shaffer v. Saffle*, 148 F.3d 1180 (10th Cir. 1998); *Rise v. Oregon*, 59 F.3d 1556 (9th Cir. 1995); *Jones v. Murray*, 962 F.2d 302 (4th Cir. 1992).

federal prisoners convicted of a variety of violent crimes, 42 U.S.C. 14135a. The Act enlarges the predicate offense list to include any crime of violence or any terrorism offense, section 503.¹³⁶

Access to Educational Records. Finally, the Act calls for an ex parte court order procedure under which senior Justice Department officials may seek authorization to collect educational records relevant to an investigation or prosecution of a crime of terrorism, section 507 (as an exception to the confidentiality requirements of the General Education Provisions Act, 20 U.S.C. 1232g), section 508 (as an exception to the confidentiality requirements of the National Education Statistics Act, 20 U.S.C. 9007).

Statute of Limitations. Prosecution for murder in violation of federal law may be initiated at any time, 18 U.S.C. 3281. A five year statute of limitations applied for most other federal crimes before passage of the Act, with a few exceptions. Among the relevant exceptions were an eight year statute of limitations for several terrorist offenses, 18 U.S.C. 3286,¹³⁷ and a ten year statute of limitations for a few arson and explosives offenses, 18 U.S.C. 3295. The Justice Department recommended the elimination of a statute of limitations in terrorism cases.¹³⁸

¹³⁶ Summarizing the law in place at the time, the Department of Justice argued that, “The statutory provisions governing the collection of DNA samples from convicted federal offenders (42 U.S.C. §14135a(d)) are restrictive, and do not include persons convicted for the crimes that are most likely to be committed by terrorists. DNA samples cannot now be collected even from persons federally convicted of terrorist murders in most circumstances. For example, 49 U.S.C. §46502, which applies to terrorists who murder people by hijacking aircraft, 18 U.S.C. §844(i), which applies to terrorists who murder people by blowing up buildings, and 18 U.S.C. 2332, which applies to terrorists who murder U.S. nationals abroad, are not included in the qualifying federal offenses for purposes of DNA sample collection under existing law. This section addresses the deficiency of the current law in relation to terrorists by extending DNA sample collection to all persons convicted of terrorism crimes,” *DoJ* at §353.

For a general discussion, see, Fischer, *DNA Identification: Applications and Issues*, CRS REP.NO. RL30717 (Jan. 12, 2001).

¹³⁷ 18 U.S.C. 32 (destruction of aircraft or aircraft facilities), 37 (violence at international airports), 112 (assaults on foreign dignitaries), 351 (crimes of violence against Members of Congress), 1116 (killing foreign dignitaries), 1203 (hostage taking), 1361 (destruction of federal property), 1751 (crimes of violence against the President), 2280 (violence against maritime navigation), 2281 (violence on maritime platforms), 2332 (terrorist violence against Americans overseas), 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), 2340A (torture); 49 U.S.C. 46502 (air piracy), 46504 (interference with a flight crew), 46505 (carrying a weapon aboard an aircraft), and 46506 (assault, theft, robbery, sexual abuse, murder, manslaughter or attempted murder or manslaughter in the special aircraft jurisdiction of the United States).

¹³⁸ “This section amends 18 U.S.C. §3286 to provide that terrorism of offenses may be prosecuted without limitation of time. This will make it possible to prosecute the perpetrators of terrorist acts whenever they are identified and apprehended.

“This section expressly provides that it is applicable to offenses committed before the date of enactment of the statute, as well as those committed thereafter. This retroactivity provision ensures that no limitation period will bar the prosecution of crimes committed in

The Act takes less dramatic action in section 809. It eliminates the statute of limitations for any crime of terrorism¹³⁹ that risks or results in a death or serious bodily injury, 18 U.S.C. 3286. In the absence of such a risk or result, all other terrorism offenses become subject to the eight year statute of limitations unless already covered by the ten year statute for explosives and arson offenses, 18 U.S.C. 3286.

Application of the statute of limitations rarely provokes a constitutional inquiry. Nevertheless, due process precludes prosecution when it can be shown that pre-indictment delay “caused substantial prejudice to [a defendant’s] rights to a fair trial and that the delay was an intentional device to gain tactical advantage over the accused.”¹⁴⁰ Moreover, a judicial difference of opinion has appeared in those cases

connection with the September 11, 2001 terrorist attacks. The constitutionality of such retroactive applications of changes in statutes of limitations is well-settled. See, e.g., *United States v. Grimes*, 142 F.3d 1342, 1350-51 (11th Cir. 1998); *People v. Frazer*, 982 P.2d 180 (Cal. 1999).

“Existing federal law (18 U.S.C. §3282) bars prosecuting most offenses after five years. 18 U.S.C. §3286, as currently formulated, extends the limitation period for prosecution for certain offenses that may be committed by terrorists – but only to eight years. While this is a limited improvement over the five-year limitation period for most federal offenses, it is patently inadequate in relation to the catastrophic human and social costs that frequently follow from such crimes as destruction of aircraft (18 U.S.C. §32), aircraft hijackings ([49] U.S.C. §§46502, 46504-06, attempted political assassinations (18 U.S.C. §§351, 1116, 1751), or hostage taking (18 U.S.C. §1203). These are not minor acts of misconduct which can properly be forgiven or forgotten merely because the perpetrator has avoided apprehension for some period of time. Anomalously, existing law provides longer limitation periods for such offenses as bank frauds and certain artwork thefts (18 U.S.C. §§3293-94) than it does for crimes characteristically committed by terrorists.

“In many American jurisdictions, the limitation periods for prosecution for serious offenses are more permissible than those found in federal law, including a number of states which have no limitation period for the prosecution of felonies generally. While this section does not go so far, it does eliminate the limitation period for prosecution of the major crimes that are most likely to be committed by terrorists (‘Federal terrorism offenses’), as specified in section 309 of this bill,” *DoJ* at 301.

¹³⁹ As defined by 18 U.S.C. 2332b(g)(5)(B), with the amendments of §808, this includes, in addition to the offenses already listed in 18 U.S.C. 3296 – 18 U.S.C. 81 (arson within U.S. special maritime and territorial jurisdiction); 175 & 175b (biological weapons); 229 (chemical weapons); 831 (nuclear weapons); 842(m) & (n) (plastic explosives); 844(f)(bombing federal property where death results); 844(i)(bombing property used in interstate commerce); 930(c)(possession of a firearm in a federal building where death results), 956(a)(conspiracy within the U.S. to commit murder, kidnapping, or to maim overseas); 1030(a) (1), (5)(A)(i), (5)(B)(ii)-(v)(computer abuse); 1114 (killing federal officers or employees); 1362 (destruction of communications facilities); 1363 (malicious mischief within the U.S. special maritime and territorial jurisdiction); 1366(a)(destruction of an energy facility); 1992 (train wrecking); 1993 (terrorist attack on mass transit); 2155 (destruction of national defense materials); 2339 (harboring terrorists); 2339A (material support to terrorists), 2339B (material support to terrorist organizations); 42 U.S.C. 2284 (sabotage of nuclear facilities); and 49 U.S.C. 60123(b)(destruction of pipeline facilities).

¹⁴⁰ *United States v. Marion*, 404 U.S. 307, 325 (1971); *United States v. Lovasco*, 431 U.S. 783, 790 (1977).

when an existing period of limitation is enlarged legislatively and the new period made applicable to past offenses. The lower federal courts have long noted that the Constitution poses no impediment to enlarging a period of limitation *as long as it does not revive an expired period*.¹⁴¹ Recently, however, the California Supreme Court held that retroactive revival of an expired statute of limitations offended neither the California nor the United States Constitution.¹⁴²

Section 809 applies “to the prosecution of any offense committed before, on, or after the date of enactment of this section,” the very words used in the Justice Department proposal. The Justice Department, in describing its proposal, cited both federal law (*Grimes*, where the court held that extensions may be applied where the earlier period of limitations has not expired) and California law (*Frazer*, where the court held that extensions may revive an expired period of limitations). The implication is that the Justice Department understood its proposal to apply to past offenses whether the earlier statute of limitations had expired or not. Other than its use of identical terminology, Congress gave no hint of whether it intended to adopt this view for section 809. Whether the federal courts could be persuaded to overcome their previously expressed constitutional reservations is equally uncertain.

Extraterritoriality. Crime is usually outlawed, prosecuted and punished where it is committed. In the case of the United States, this is ordinarily a matter of practical and diplomatic preference rather than constitutional necessity. Consequently, although prosecutions are somewhat uncommon, a surprising number of federal criminal laws have extraterritorial application. In some instances, the statute proscribing the misconduct expressly permits the exercise of extraterritorial jurisdiction, 18 U.S.C. 2381 (treason) (“Whoever, owing allegiance to the United States . . . within the United States or elsewhere. . .”). In others, such as those banning assassination of Members of Congress, 18 U.S.C. 351, or the murder of federal law enforcement officers, 18 U.S.C. 1114, the courts have assumed Congress intended the prohibitions to have extraterritorial reach.¹⁴³

The Act touches upon extraterritoriality only to a limited extent and in somewhat unusual ways. Congress has made most common law crimes – murder, sexual abuse, kidnaping, assault, robbery, theft and the like – federal crimes when committed within the special maritime and territorial jurisdiction of the United States. The special maritime and territorial jurisdiction of the United States represents two variations of extraterritorial jurisdiction.

¹⁴¹ *United States v. De La Matta*, 266 F.3d 1275, 1286 (11th Cir. 2001); *United States v. Grimes*, 142 F.3d 1342, 1351 (11th Cir. 1998); *United States v. Morrow*, 177 F.3d 272, 294 (5th Cir. 1999); *Falter v. United States*, 23 F.2d 420, 425-26 (2d Cir. 1928).

¹⁴² *People v. Frazer*, 24 Cal.4th 737, 759, 982 P.2d 180, 1294, 88 Cal.Rptr.2d 312, 327 (1999).

¹⁴³ *United States v. Layton*, 855 F.2d 1388 (9th Cir. 1988)(at the time of the overseas murder of Congressman Ryan for which Layton was convicted the statute was silent as to its extraterritorial application; several years later Congress added an explicit extraterritorial provision, 18 U.S.C. 351(i)); *United States v. Benítez*, 741 F.2d 1312 (11th Cir. 1984)(18 U.S.C. 1114 has since expanded to protect all federal officers and employees, including members of the armed forces and those assisting them).

The special maritime jurisdiction of the United States extends to the vessels of United States registry. Historically, the territorial jurisdiction of the United States was thought to reach those areas over which Congress enjoyed state-like legislative jurisdiction. For some time, those territories were located exclusively within the confines of the United States, but over the years they came to include at least temporarily, Hawaii, the Philippines, and several other American overseas territories and possessions. Recently, the lower federal courts have become divided over the question of whether laws, enacted to apply on federal enclaves within the United States and within American territories overseas, might also apply to areas in foreign countries over which the United States has proprietary control.¹⁴⁴

The Act resolves the conflict by declaring within the territory of the United States those overseas areas used by American governmental entities for their activities or residences for their personnel, at least to the extent that crimes are committed by or against an American, section 804 (18 U.S.C. 7 (9)). The section is inapplicable where it would otherwise conflict with a treaty obligation or where the offender is covered by the Military Extraterritorial Jurisdiction Act, 18 U.S.C. 3261.

Victims. Federal law has provided for crime victim compensation and assistance programs for some time. Moreover, Congress enacted September 11th Victim Compensation Fund legislation before it passed the Act. Consequently, the Act's victim provisions focus on adjustments to existing programs, primarily to those of the Victims of Crime Act of 1984, 42 U.S.C. 10601 *et seq.*, and to those maintained for the benefit of public safety officers and their survivors, 42 U.S.C. 3796 *et seq.*

Public safety officers - police officers, firefighters, ambulance and rescue personnel - killed or disabled in the line of duty (and their heirs) are entitled to federal benefits. Prior to the Act, death benefits were set at \$100,000 and the total amount available for disability benefits in a given year was capped at \$5 million, 42 U.S.C. 3796 (2000 ed.). No benefits could be paid for suicides, if the officer was drunk or grossly negligent, if the beneficiary contributed to the officer's death or injury, or if the officer were employed other than in a civilian capacity, 42 U.S.C. 3796 (2000 ed.). The Act increases the death benefit to \$250,000 (retroactive to January 1, 2001), section 613; and for deaths and disability connected with acts of terrorism waives the \$5 million disability cap and the disqualifications for gross negligence, contributing cause, or employment in a noncivilian capacity, section 611.

Most of fines collected for violation of federal criminal laws are deposited in the Crime Victims Fund which is available for child abuse prevention and treatment grants, victim services within the federal criminal justice system, and grants to state victim compensation and victim assistance programs, 42 U.S.C. 10601 to 10608. The Act:

¹⁴⁴ Compare, *United States v. Gatlin*, 216 F.3d 207 (2d Cir. 2000); *United States v. Laden*, 92 F.Supp.2d 189 (S.D.N.Y. 2000); with, *United States v. Corey*, 232 F.3d 1166 (9th Cir. 2000); *United States v. Erdos*, 474 F.2d 157 (4th Cir. 1973).

- authorizes private contributions to the fund (42 U.S.C. 10601(b)), section 621(a)
- instructs the Department of Justice, which administers the fund, to distribute in every fiscal year (if amounts in the Fund are sufficient) amounts equal to between 90% and 110% of the amount distributed in the previous fiscal year (120% in any year when the amount on hand is twice the amount distributed the previous year)(42 U.S.C. 10601(c)), section 621(b)
- reduces by 1% the amounts available for compensation and assistance grants (from 48.5% to 47.5% after child abuse and federal victim priorities have been met), and increases from 3% to 5% the amount available for Justice Department discretionary spending for demonstration projects and services to assist the victims of federal crimes (42 U.S.C. 10601(d), 10603(c)), section 621(c)
- converts the general reserve fund to an antiterrorism reserve fund and reduces the cap on the reserve from \$100 million to \$50 million (42 U.S.C. 10601(d)(5)), section 621(d)
- waives the Fund's availability caps with respect to funds transferred to it in response to the terrorist attacks of September 11 (42 U.S.C. 10601 note)), section 621(e)
- lowers the annual reduction rate on individual compensation program grants; beginning in 2003 individual grants are limited to 60% (rather than 40%) of the amount of awarded in the previous year (42 U.S.C. 10602(a)), section 622(a)
- eliminates the requirement that state compensation programs permit compensation for state residents who are the victims of terrorism overseas (42 U.S.C. 10602(b)(6)(B)), section 622(b)
- provides that compensation under the September 11th Victim Compensation Fund should be counted as income in considering eligibility for any federal indigent benefit program (42 U.S.C. 10602(c)), section 622(c)
- drops "crimes involving terrorism" from the definition of "compensable crime"; it is unclear whether the phrase was removed as redundant or pursuant to a determination to compensate victims other than through the Crime Victims Fund (42 U.S.C. 10602(d)), section 622(d)(1)
- makes it clear that the Virgin Islands is eligible to receive grants (42 U.S.C. 10602(d)), section 622(d)(2)
- adds the September 11th Victim Compensation Fund to the "double dipping" restriction that applies to the victim compensation programs and confirms that state compensation programs will not be rendered ineligible for grants by virtue of a refusal to pay dual compensation to September 11th Fund victims (42 U.S.C. 10602(e)), section 622(e)

- makes federal agencies performing law enforcement functions in the District of Columbia, Puerto Rico, the Virgin Islands, and other U.S. territories and possessions eligible for victim assistance grants (42 U.S.C. 10603(a)(6)), section 623(a)
- prohibits program discrimination against crime victims based on their disagreement with the manner in which the state is prosecuting the underlying offense (42 U.S.C. 10603(b)(1)(F)), section 623(b)
- allows Justice Department discretionary grants for purposes of program evaluation and compliance and for fellowships, clinical internships and training programs (42 U.S.C. 10603(c)(1)(A), (3)(E)), section 623(c),(e)
- reverses the preference for victim service grants over demonstration projects and training grants, so that *not more* than 50% of the amounts available for crime victim assistance grants shall be used for victim service grants and *not less* than 50% for demonstration projects and training grants (42 U.S.C. 10603(c)(2)), section 623(d)
- makes federal and local agencies and private entities eligible for supplemental grants for services relating to victims of terrorism committed within the U.S. (42 U.S.C. 10603b(b)), section 624(a)
- allows supplemental grants for services relating to victims of terrorism committed overseas regardless of whether the victims are eligible for compensation under Title VIII of the Omnibus Diplomatic Security and Antiterrorism Act (100 Stat. 879 (1986))(Title VIII victims were previously ineligible) (42 U.S.C. 10603b(a)(1)), section 624(b)
- establishes a “double dipping” restriction under which compensation to the victims of overseas terrorism is reduced by the amount received under Title VIII of the Omnibus Act (42 U.S.C. 10603c(b)), section 624(c)

Increasing Institutional Capacity. A major portion of the Act is devoted to bolstering the institutional capacity of federal law enforcement agencies to combat terrorism and other criminal threats. In addition to the counterterrorism discussed above in the context of the Attorney General's reward prerogatives, it increases funding authorization for an FBI technical support center, section 103, and allows the FBI to hire translators without regard to otherwise applicable employment restrictions such as citizenship, section 205.

In the area of cybercrime, the Attorney General is instructed to establish regional forensic laboratories, section 817, and the Secret Service, to establish a national network of electronic crime task forces, modeled after its New York Electronic Crimes Task Force, section 105. The Act likewise clarifies the Secret Service's investigative jurisdiction with respect to computer crime (18 U.S.C. 1030) and to crimes involving credit cards, PIN numbers, computer passwords, or any frauds against financial institutions (18 U.S.C. 3056), section 506.

For a period of up to 180 days after the end of Operation Enduring Freedom, section 1010 allows the Department of Defense (DoD) to contract with state and local law enforcement authorities to perform various security functions on its military installations and facilities, 10 U.S.C. 2465.

The Act also authorizes appropriations for wide range anti-terrorism purposes including:

- \$25 million a year for FY 2003 through FY 2007 for state and local terrorism prevention and antiterrorism training grants for first responders, section 1005 (28 U.S.C. 509 note)
- necessary sums (FY 2002 through FY 2007) for Office of Justice Programs (OJP) grants to state and local governments to enhance their capacity to respond to terrorist attacks, section 1014 (42 U.S.C. 3711)
- \$250 million a year (FY 2002 through FY 2007) for OJP grants to state and local governments integrated information and identification systems, section 1015 (42 U.S.C. 14601)
- \$50 million per fiscal year for the Attorney General to develop and support regional computer forensic laboratories (28 U.S.C. 509 note), section 816
- \$50 million (FY 2002) and \$100 million (FY 2003) for Bureau of Justice Assistance grants (42 U.S.C. 3796h) for federal-state-local law enforcement information sharing systems, section 701
- \$20 million (FY 2002) for the activities of National Infrastructure Simulation and Analysis Center in DoD's Defense Threat Reduction Agency, section 1016 (42 U.S.C. 5195c)
- \$5 million for DEA police training in South and Central Asia, section 1007.

Miscellaneous. Finally, the Act addresses the issuance of licenses for the drivers of vehicles carrying hazardous materials and the use of trade sanctions against countries that support terrorism.

The Act requires background checks for criminal records and immigration status of applicants for licenses to operate vehicles carrying hazardous materials including chemical and biological materials (49 U.S.C. 5101a), section 1012.

The Trade Sanctions Reform and Export Enhancement Act, 22 U.S.C. 7201 to 7209, limits the President's authority to unilaterally impose export restrictions on food and medical supplies. The limitations do not apply to restrictions on products that might be used for the development or production of chemical or biological weapons or of weapons of mass destruction, 22 U.S.C. 7203(2)(c). The Act expands the exception to include products that might be used for the *design* of chemical or biological weapons or of weapons of mass destruction as well, section 221(a)(1).

Only one year licenses may be issued for trade with countries that sponsor terrorism, 22 U.S.C. 7205. The Act brings areas of Afghanistan controlled by the Taliban within the same restriction, section 221(a)(2).

Neither of these changes or anything else in the trade sanctions legislation precludes the assessment of civil or criminal liability for violations of 18 U.S.C. 2339A (providing support to terrorists), of 18 U.S.C. 2339B (providing support to terrorist organizations), or of various presidential orders under the International Emergency Economic Powers Act,¹⁴⁵ or of restrictions on foreign involvement in weapons of mass destruction or missile proliferation, sections 221(b), 807.¹⁴⁶

¹⁴⁵ *I.e.*, Executive Order No. 12947, 50 U.S.C. 1701 note (prohibiting transactions with terrorists); Executive Order No. 13224, 50 U.S.C. 1701 note (blocking property of persons who support terrorism); Executive Order No. 12978, 50 U.S.C. 1701 note (blocking assets of significant narcotics traffickers).

¹⁴⁶ For a general discussion of trade sanctions legislation, *see*, Jurenas, *Exempting Food and Agriculture Products from U.S. Economic Sanctions: Status and Implementation*, CRS ISSUE BRIEF IB100061.

September 9, 2003

Honorable Patrick J. Leahy
Committee on the Judiciary
United States Senate
Washington, DC 20510

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-14-2005 BY 65179/DMH/LP/RW 05-cv-0845

Dear Senator Leahy:

I am writing in response to your letter to Director Mueller dated July 25, 2003 regarding information on the FBI's website relating to access to library records under Section 215 of the USA PATRIOT Act.

After receiving your letter, we reviewed the portion of the website about which you raised concerns. In doing so, we identified an error relating to the standard of proof for obtaining an order from the Foreign Intelligence Surveillance Court. We have deleted the statement that:

the FBI must prove to a judge that it has probable cause and must certify to the court that these records are sought for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

We replaced that language with the statement that:

the FBI must certify that these records are relevant for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

1 - Mr. Wainstein
1 - Ms. Chandler
1 - Ms. Caproni
① - Mr. Rowan
1 - Mr. Bowman

1 - Ms. Kalisch
1 - OCA Member's Folder
1 - Exec Sec
EPK:crm(10)

b6

b7C

Rowan, J Patrick

From: [REDACTED]
Sent: Wednesday, September 10, 2003 2:16 PM
To: Rowan, J Patrick
Cc: KALISCH, ELENI P. [REDACTED]
Subject: SSCI Member Briefing on 09/11/2003 @ 2:30 p.m.: Patriot Act

b6

Pat,

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-14-2005 BY 65179/DMH/LP/RW 05-cv-0845

b7C

I attended the Pre-Brief at DOJ and provide the following in summary:

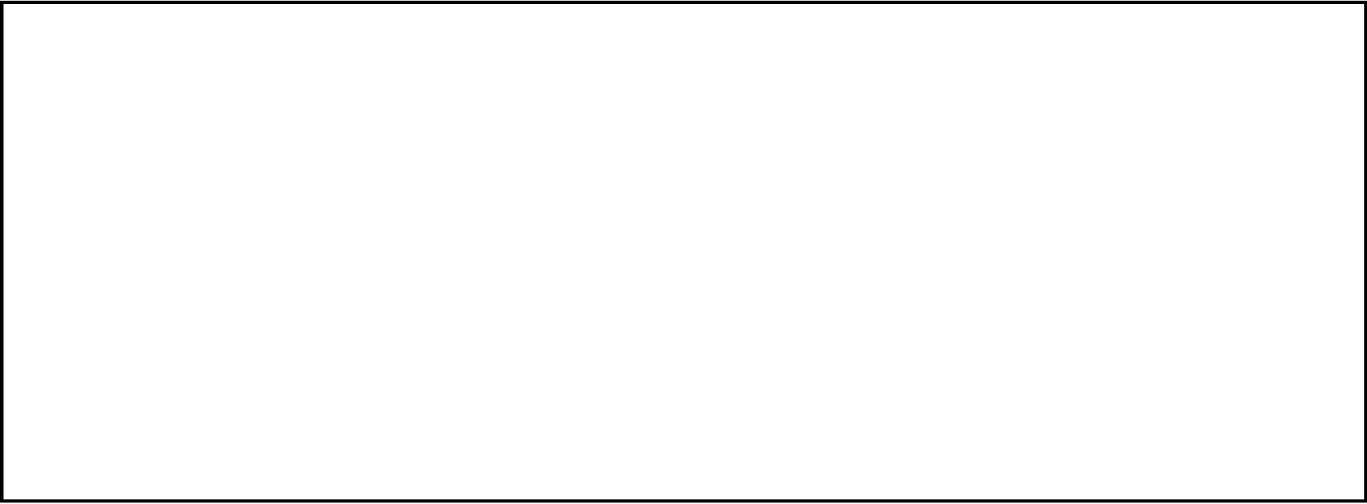
[REDACTED]

b6

b7C

b5

[REDACTED]



b2
b6
b7C
b5

Section 215 of the USA PATRIOT Act

"The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."

House Judiciary Committee press release,
October 17, 2002

50 U.S.C. § 1861. Access to certain business records for foreign intelligence and international terrorism investigations.

(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) Each application under this section

(1) shall be made to—

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in

→ **Comparable to Grand Jury Power:** For years, grand juries have issued subpoenas to all types of entities, including libraries and bookstores.

- In a recent **domestic-terrorism** case, a grand jury served a subpoena to a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.
- In the **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.
- In the **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a Manhattan library. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.

→ **First Amendment Rights:** Section 215 goes to great lengths to preserve the First Amendment rights of those who are under investigation, including the patrons of libraries and bookstores. FBI agents are prohibited from using a suspect's exercise of First Amendment rights as a pretext for seeking records or information.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-CV-0845

→ **Narrow Scope:** Section 215 can only be used in a narrow set of investigations: (1) to obtain foreign intelligence information about people who are neither American citizens nor lawful permanent residents; or (2) to defend the United States against spies or international terrorists. Section 215 cannot be used to investigate garden-variety crimes, or even domestic terrorism.

→ **Court Order Requirement:** FBI agents cannot obtain records under section 215 unless they receive a court order. Agents cannot use this authority unilaterally to compel libraries or any other entity to turn over their records. They can obtain such documents only by appearing before the FISA court and convincing it that they need them.

subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1862. Congressional oversight.

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 1861 of this title.

(b) On a semiannual basis, the attorney general shall provide to the committees on the judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

(1) the total number of applications made for orders approving requests for the production of tangible things under section 1861 of this title; and

(2) the total number of such orders either granted, modified, or denied.

→ **Confidentiality Comparable to Other Laws:** The requirement that recipients of court orders keep them confidential is based on the “national security letter” statutes, which have existed for decades. (An NSL is a type of administrative subpoena used in certain national-security investigations.)

- 12 U.S.C. § 3414(a)(5)(D): “No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph.”
- 18 U.S.C. § 2709(c): “No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.”

→ **Oversight:** Section 215 provides for thorough congressional oversight. Every six months, the Attorney General is required to “fully inform” Congress on the number of times agents have sought a court order under section 215, as well as the number of times such requests were granted, modified, or denied.

Rowan, J Patrick

From: [REDACTED]
Sent: Thursday, July 10, 2003 11:58 AM
To: Rowan, J Patrick; Rosenberg, Charles P
Subject: RE: Libraries

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-14-2005 BY 65179/DMH/LP/RW 05-cv-0845

b6

b7C

b5

-----Original Message-----

From: Rowan, J Patrick
Sent: Thursday, July 10, 2003 10:59 AM
To: [REDACTED] Rosenberg, Charles P
Subject: RE: Libraries

b6

b7C

-----Original Message-----

From: [REDACTED]
Sent: Thursday, July 10, 2003 10:52 AM
To: Rosenberg, Charles P; Rowan, J Patrick
Subject: RE: Libraries

b5

b6

b7C

b5

b6

b7C

Chuck & Pat,

[REDACTED]

Hope this helps.

b5

b6

[REDACTED]

-----Original Message-----

From: Rosenberg, Charles P
Sent: Thursday, July 10, 2003 5:51 AM
To: Rowan, J Patrick
Cc: [REDACTED]
Subject: RE: Libraries

b5

b6

b7C

[REDACTED]

-----Original Message-----

From: Rowan, J Patrick
Sent: Wednesday, July 09, 2003 6:09 PM
To: Rosenberg, Charles P
Subject: RE: Libraries

[REDACTED]

-----Original Message-----

From: Rosenberg, Charles P
Sent: Wednesday, July 09, 2003 5:17 PM
To: Rowan, J Patrick
Cc: Wainstein, Kenneth L
Subject: Libraries

b5

b6

b7C

Pat: [REDACTED]

[REDACTED]

Section 215 of the USA PATRIOT Act

"The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/Lp/RW 05-cv-0845

House Judiciary Committee press release,
October 17, 2002

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

"(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

"(2) An investigation conducted under this section shall—

"(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

"(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

"(b) Each application under this section—

"(1) shall be made to—

"(A) a judge of the court established by section 103(a); or

"(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

"(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

"(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

"(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

► **Comparable to Grand Jury Power:** For years, grand juries have issued subpoenas to all types of entities, including libraries and bookstores.

- In a recent **domestic-terrorism** case, a grand jury served a subpoena to a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.
- In the **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.
- In the **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a Manhattan library. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.

► **First Amendment Rights:** Section 215 goes to great lengths to preserve the First Amendment rights of those who are under investigation, including the patrons of libraries and bookstores. FBI agents are prohibited from using a suspect's exercise of First Amendment rights as a pretext for seeking records or information.

► **Narrow Scope:** Section 215 can only be used in a narrow set of investigations: (1) to obtain foreign intelligence information about people who are neither American citizens nor lawful permanent residents; or (2) to defend the United States against spies or international terrorists. Section 215 cannot be used to investigate garden-variety crimes, or even domestic terrorism.

► **Court Order Requirement:** FBI agents cannot obtain records under section 215 unless they receive a court order. Agents cannot use this authority unilaterally to compel libraries or any other entity to turn over their records. They can obtain such documents only by appearing before the FISA court and convincing it that they need them.

“(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

“(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

“SEC. 502. CONGRESSIONAL OVERSIGHT.

“(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

“(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

“(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

“(2) the total number of such orders either granted, modified, or denied.”

→ **Confidentiality Comparable to Other Laws:** The requirement that recipients of court orders keep them confidential is based on the “national security letter” statutes, which have existed for decades. (An NSL is a type of administrative subpoena used in certain national-security investigations.)

- 12 U.S.C. § 3414(a)(5)(D): “No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer’s or entity’s financial records under this paragraph.”
- 18 U.S.C. § 2709(c): “No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.”

→ **Oversight:** Section 215 provides for thorough congressional oversight. Every six months, the Attorney General is required to “fully inform” Congress on the number of times agents have sought a court order under section 215, as well as the number of times such requests were granted, modified, or denied.

United States District Court Eastern District of Michigan



Summons in a Civil Action and Return of Service Form

DENISE PAGE HOOD

03-72913

MAGISTRATE JUDGE R. STEVEN WHALEN
Plaintiff(s) Name

Case Number and Judge Assignment (to be supplied by the Court)

MUSLIM COMMUNITY ASSOCIATION OF
ANN ARBOR, et al. (SEE ATTACHMENT FOR
REMAINDER OF PLAINTIFFS)

Defendant(s) Name

JOHN ASHCROFT, in his official capacity as
Attorney General of the United States; ROBERT
MUELLER, in his official capacity as Director of
the Federal Bureau of Investigation,

Plaintiffs attorney, address and telephone:

Ann Beeson/Jameel Jaffer, ACLU Foundation, 125
Broad Street, 18th Floor, New York, NY
10004-2400, (212) 549-2500; Michael J.
Steinberg, Noel Saleh, Kary L. Moss, ACLU of
Michigan, 60 W. Hancock, Detroit, MI 48201;
(313)-578-6800

Name and address of defendant being served:

ROBERT MUELLER, Director
Federal Bureau of Investigation
935 Pennsylvania Ave., NW
Washington, D.C. 20535

To the defendant

This summons is notification that YOU ARE BEING SUED by the above named plaintiff(s).

1. You are required to serve upon the plaintiff's attorney, name and address above, an answer to the complaint within 60 days after receiving this summons, or take other actions that are permitted by the Federal Rules of Civil Procedure.
2. You must file the original and one copy of your answer within the time limits specified above with the Clerk of Court.
3. Failure to answer or take other action permitted by the Federal Rules of Civil Procedure may result in the issuance of a judgment by default against you for the relief demanded in the complaint.

David J. Weaver
Clerk of the Court

By:

Deputy Clerk



b6

b7C

For Your Info

**From
Pat Kelley**

JUL 30 2003

Date of issuance

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

MUSLIM COMMUNITY ASSOCIATION OF ANN
ARBOR; AMERICAN-ARAB ANTI-DISCRIMINATION
COMMITTEE; ARAB COMMUNITY CENTER FOR
ECONOMIC AND SOCIAL SERVICES; BRIDGE
REFUGEE & SPONSORSHIP SERVICES, INC.;
COUNCIL ON AMERICAN-ISLAMIC RELATIONS;
ISLAMIC CENTER OF PORTLAND, MASJED
AS-SABER,

Plaintiffs,

v.

JOHN ASHCROFT, in his official capacity as Attorney
General of the United States; ROBERT MUELLER, in his
official capacity as Director of the Federal Bureau of
Investigation,

Defendants.

ANN BEESON
JAMEEL JAFFER
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500

MICHAEL J. STEINBERG
NOEL SALEH
KARY L. MOSS
American Civil Liberties Union Fund of Michigan
60 West Hancock
Detroit, MI 48201-1343
(313) 578-6800

Attorneys for Plaintiffs

03-72913
COMPLAINT FOR
DECLARATORY AND
INJUNCTIVE RELIEF

DENISE PAGE HOOD

Case No.

MAGISTRATE JUDGE R. STEVEN WHALE
Hon.

U.S. DIST. COURT CLERK
EAST DIST. MICH
DETROIT

03 JUL 30 AM 8:47

FILED

COMPLAINT

PRELIMINARY STATEMENT

1. This lawsuit challenges the constitutionality of Section 215 of the USA PATRIOT Act, which vastly expands the power of the Federal Bureau of Investigation ("FBI") to obtain records and other "tangible things" of people not suspected of criminal activity. Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) ("Patriot Act" or "Act"). The FBI can use Section 215 to obtain personal belongings, including "books, records, papers, documents, and other items," directly from a person's home. It can also order charities, political organizations, libraries, hospitals, Internet Service Providers, or indeed *any* person or entity to turn over the records or personal belongings of others. The FBI can use Section 215 against anyone at all, including United States citizens and permanent residents.

2. Section 215 is invalid on its face. To obtain a Section 215 order, the FBI need only assert that the records or personal belongings are "sought for" an ongoing foreign intelligence, counterintelligence, or international terrorism investigation. The FBI is not required to show probable cause – or any reason – to believe that the target of the order is a criminal suspect or foreign agent. The FBI can obtain and execute Section 215 orders in total secrecy. The targets of Section 215 orders are *never* notified that their privacy has been compromised – even years later, and even if they are innocent. The law includes a gag provision that prohibits persons or entities served with Section 215 orders from ever disclosing, even in the most general terms, that the FBI has sought information from them. By seriously compromising the rights to privacy, free speech, and due process, Section 215 violates the First, Fourth, and Fifth Amendments of the United

States Constitution. Plaintiffs respectfully seek a declaration that Section 215 is facially unconstitutional, and a permanent injunction against its enforcement.

JURISDICTION AND VENUE

3. This case arises under the United States Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the United States Constitution and 28 U.S.C. § 1331. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.* The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412. Venue is proper in this district under 28 U.S.C. § 1391(e).

PARTIES

4. Plaintiff Muslim Community Association of Ann Arbor ("MCA") is a non-profit, membership-based organization that serves the religious needs of Muslims in and around Ann Arbor, Michigan. MCA owns and administers a mosque and an Islamic school. MCA sues on its own behalf and on behalf of its members, students, and constituents.

5. Plaintiff American-Arab Anti-Discrimination Committee ("ADC") is a non-profit civil rights organization committed to defending the rights of people of Arab descent and promoting their rich cultural heritage. ADC, which is non-sectarian and non-partisan, is the largest Arab-American grassroots organization in the United States. Based in Washington, D.C., it was founded in 1980 by former United States Senator James Abourezk and has chapters nationwide. ADC sues on its own behalf and on behalf of its members and constituents.

6. Plaintiff Arab Community Center for Economic and Social Services (“ACCESS”) is a Detroit-based human services organization committed to the development of the Arab-American community in all aspects of its economic and cultural life. Among other services, ACCESS operates a Community Health and Research Center. ACCESS sues on its own behalf and on behalf of its members, clients, and constituents.

7. Plaintiff Bridge Refugee & Sponsorship Services, Inc. (“Bridge”) is an ecumenical, non-profit organization based in Knoxville, Tennessee, dedicated to helping refugees and asylum-seekers become and stay self-sufficient. Bridge is affiliated with Church World Service and with Episcopal Migration Ministries. Bridge recruits and trains church sponsors to help refugees create new lives in East Tennessee, and provides services until refugees are eligible to apply for United States citizenship. Bridge sues on its own behalf and on behalf of its clients.

8. Plaintiff Council on American Islamic Relations (“CAIR”) is a non-profit, mainstream, grassroots organization dedicated to enhancing the public’s understanding of Islam and Muslims. CAIR is the largest Islamic civil liberties organization in the United States. CAIR is based in Washington, D.C., and has chapters nationwide and in Canada. CAIR sues on its own behalf and on behalf of its members and constituents.

9. Plaintiff Islamic Center of Portland, Masjed As-Saber (“ICPMA”), is a non-profit organization that serves the religious needs of Muslims in and around Portland, Oregon. ICPMA owns and administers a mosque known as Masjed As-Saber and an Islamic school known as the Islamic School of Portland. ICPMA sues on its own behalf and on behalf of its community members and students.

10. Defendant Attorney General John Ashcroft heads the United States Department of Justice, which is the agency of the United States government responsible for enforcement of federal criminal laws and domestic intelligence investigations. Defendant Attorney General Ashcroft has ultimate authority for supervising all of the operations and functions of the Department of Justice. The Department of Justice includes the FBI, the agency authorized to use the law challenged in this case.

11. Defendant Robert Mueller is the Director of the FBI, which is the principal investigative arm of the United States Department of Justice. Defendant Robert Mueller is responsible for supervising all of the operations and functions of the FBI. The FBI is the agency authorized to use the law challenged in this case.

STATUTORY LANGUAGE AT ISSUE

12. The Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, was enacted in 1978 to govern FBI surveillance of foreign powers and their agents inside the United States. *See* Pub. L. 95-511, 92 Stat. 1783 (Oct. 25, 1978). Through FISA, Congress created the Foreign Intelligence Surveillance Court ("FISA Court"), originally composed of seven (now eleven) federal district judges empowered to grant or deny government applications for FISA surveillance orders. *See* 50 U.S.C. § 1803.

13. Since 1978, Congress has amended FISA numerous times, each time adding new tools to the FBI's foreign intelligence toolbox or expanding the class of investigations in which such tools may be employed.

14. One amendment, which was codified as Subchapter IV of FISA, authorized the FBI to obtain "business records" from vehicle rental agencies, common carriers, storage facilities, and other similar businesses if the FBI had "specific and

articulable facts” giving reason to believe that the records in question pertained to a foreign agent or power. *See* Pub. L. 105-272, Title VI, § 602, 112 Stat. 2411 (Oct. 20, 1998).

15. The Patriot Act was passed on October 26, 2001.

16. Section 215 of the Patriot Act amended Subchapter IV of FISA by:

(i) allowing the FBI to demand the production of “any tangible things (including books, records, papers, documents, and other items),” and not just business records; (ii) allowing the FBI to demand books, records and other tangible things from *anyone*, and not just from vehicle rental agencies and other third parties; and (iii) allowing the FBI to demand books, records and other tangible things without showing any evidence that the person whom it is investigating is a foreign agent. *See* 50 U.S.C. § 1861(a)(1).

17. Section 215 does not require the FBI to show probable cause or any reason to believe that the records or personal belongings sought pertain to a person involved in criminal activity or to a foreign agent or foreign power. *See id.* § 1861(b)(2). The provision requires only that the FBI certify to the FISA Court that the books, records, or other tangible things demanded on the authority of the provision are “sought for” a foreign intelligence, clandestine intelligence, or international terrorism investigation. As a result of the changes effected by the Patriot Act, the FBI is now authorized to use Section 215 even against people who are known to be altogether unconnected to criminal activity or espionage.

18. Section 215 requires the FISA Court to defer to the FBI’s specification that the records or personal belongings sought by a Section 215 order are sought for an investigation to obtain foreign intelligence information or to protect against international

terrorism or clandestine intelligence activities. The FISA Court has no statutory authority to examine the foundation of the FBI's specification or to reject the specification as unfounded. *See id.* § 1861(b)(2) & (c)(1).

19. Section 215 does not require the FBI to have reason to believe that the records or personal belongings sought pertain to a particular suspect or a particular offense. Accordingly, the FBI could use Section 215 to obtain from a bookstore a list of people who had purchased a particular book, or to obtain from a health clinic a list of patients who had received medical care. The FBI need not state or even know in advance which individuals' privacy will be infringed.

20. At a hearing before the House Judiciary Committee on June 5, 2003, Defendant Attorney General John Ashcroft stated that, prior to the Patriot Act, the government "used to have [to allege] a reason to believe that the target is an agent of a foreign power," a standard he agreed was "lower than probable cause." He acknowledged that, under Section 215, the government may now obtain "all relevant, tangible items" without such a showing.

21. Section 215 does not require the FBI ever to notify surveillance targets that it has obtained their records or personal belongings.

22. Section 215 does not include any procedure that would allow a person or entity served with a Section 215 order to challenge the order's constitutionality before turning over the records or personal belongings sought by the order.

23. Section 215 authorizes the FBI to obtain records or personal belongings of United States citizens and permanent residents based in part on "activities protected by the first amendment to the Constitution." *Id.* § 1861(a)(1); *see also* § 1861(a)(2)(B).

24. Section 215 authorizes the FBI to obtain records or personal belongings of people who are not United States citizens or permanent residents based *solely* upon “activities protected by the First Amendment to the Constitution.” *See id.* § 1861(a)(1); *see also* § 1861(a)(2)(B).

25. Section 215 requires the FISA Court to defer to the FBI’s specification that the investigation is not being conducted of a United States person solely upon the basis of activities protected by the First Amendment. The FISA Court has no statutory authority to examine the foundation of the FBI’s specification or to reject the specification as unfounded. *See id.* § 1861(b)(2) & (c)(1).

26. Section 215 includes the following gag provision: “No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.” *See id.* § 1861(d). Section 215 gag orders are indefinite, and do not require the FBI to make a showing that secrecy is necessary in any particular case.

27. Defendant Attorney General John Ashcroft has refused to disclose publicly even the most basic information about the FBI’s use of Section 215. He has refused to say, for example, how many times the provision has been used to obtain information from public libraries, how many times it has been used to obtain information about United States citizens or permanent residents, and how many times it has been used in response to a person’s engagement in activity protected by the First Amendment.

28. Through a request submitted under the Freedom of Information Act, the American Civil Liberties Union obtained heavily redacted documents that indicate that the FBI has already used Section 215.

29. At a June 2003 hearing, Defendant Attorney General Ashcroft informed the House Judiciary Committee that it is his position that Section 215 could be used to obtain, among other things, library and bookstore records, computer files, education records, and even genetic information.

FACTUAL BACKGROUND

30. Based on their personal experiences and the government's own actions, plaintiffs have a well-founded belief that they and their members, clients, and constituents (hereinafter "members and clients") have been or are currently the targets of investigations conducted under Section 215. Because Section 215 does not require the government to provide notice to surveillance targets, and because it strictly gags recipients from disclosing that the FBI has sought or obtained information from them, plaintiffs and other innocent targets of FBI surveillance have no way to know with certainty that their privacy has been compromised.

31. The FBI has already targeted plaintiffs, their members, and their clients in a number of ways.

32. The FBI has sought information directly from some of the plaintiffs about their members and clients.

33. The FBI has sought information from some of the plaintiffs' members and clients directly, either during visits to their homes and businesses, or through numerous

registration and interview programs directed at Muslims of Arab and South Asian descent.

34. Plaintiffs have many members and clients who were required to register under the National Security Entry-Exit Registration System (NSEERS), an INS program that thus far has been applied almost exclusively to nationals of predominantly Arab and Muslim countries. Many individuals who appeared in good faith for registration were then detained by the INS for alleged immigration violations. The FBI also interviewed many of plaintiffs' members and clients of Arab, Muslim, and South Asian descent in March 2002. Finally, the FBI interviewed many of plaintiffs' members and clients of Iraqi descent in March 2003, as part of "Operation Liberty Shield."

35. During these interviews, many members were questioned about their religious and political beliefs, activities, and associations. Some of plaintiffs' members expressed opposition to the war in Iraq, to United States support for Israeli policies, and to other aspects of United States foreign policy. Plaintiffs' members and clients believe that the FBI may have selected them for investigation under Section 215 because of information obtained during these interviews.

36. The Attorney General stated publicly in November 2002 that the Justice Department had a "previously undisclosed intelligence program involv[ing] tracking thousands of Iraqi citizens and Iraqi-Americans with dual citizenship."

37. The FBI is currently investigating a number of charities suspected of providing material support to Foreign Terrorist Organizations. Some of plaintiffs' members and clients contributed financially to these charities before the charities were accused of having provided material support.

38. Some of the plaintiffs and their members and clients have direct contacts with people whom the INS detained and the FBI interrogated after September 11th. The FBI routinely interrogated INS detainees, asking questions not only about the detainees' own immigration status, political views, religious beliefs, and foreign connections but also about the political views, religious beliefs, and foreign connections of the detainees' friends and family members.

39. Many of plaintiffs' members and clients emigrated to the United States from countries the government has accused of sponsoring terrorism, such as Syria and Iraq. Defendant Mueller has stated publicly that a "substantial" number of persons are under constant surveillance, particularly in communities like New York and Detroit, where plaintiffs have thousands of Arab-American members and clients.

40. Many of the plaintiffs directly serve Muslim communities, or have significant numbers of members or clients who are Muslim. Two of the plaintiffs, the Muslim Community Association of Ann Arbor and the Islamic Center of Portland, Masjed As-Saber, operate mosques.

41. Section 215 has caused some of plaintiffs' members and clients to be inhibited from publicly expressing their political views, attending mosque and practicing their religion, participating in public debate, engaging in political activity, associating with legitimate political and religious organizations, donating money to legitimate charitable organizations, exercising candor in private conversations, researching sensitive political and religious topics, visiting particular websites, and otherwise engaging in activity that is protected by the First Amendment to the United States Constitution.

Muslim Community Association of Ann Arbor

42. MCA is a non-profit, membership-based organization that owns and administers a mosque and an Islamic school, the Michigan Islamic Academy, in Ann Arbor, Michigan. Approximately 1000 people attend services at the mosque each Friday; as many as 2500 attend services on religious holidays. MCA employs approximately 20 people and has about 700 registered, dues-paying members.

43. Approximately 200 students are enrolled at the Michigan Islamic Academy, which offers classes from pre-K through 11th grade. In addition to offering the standard academic curriculum used in the State of Michigan for public schools, the school offers classes in Arabic language, Quranic recitation and Islamic Studies. The mission of the school is to provide students with the basic knowledge required to preserve their Islamic heritage, religion and cultural identity.

44. MCA has spent a significant amount of time, staff resources, and funds discussing the impact of September 11th and the Patriot Act on the civil rights of Muslims. It sponsored civil rights forums on January 26, 2002; April 14, 2002; October 13, 2002; and March 12, 2003. Each of these forums addressed the impact of the Patriot Act. The MCA has also sponsored numerous rallies and fundraisers related to the Rabih Haddad case; at these events, the Patriot Act was almost always discussed.

45. Because of the relationship between MCA, its members and leaders, and persons and organizations investigated, questioned, detained, or arrested since September 11th, MCA reasonably believes that the FBI has used or is currently using Section 215 to obtain records or personal belongings about it and its members, students, and constituents.

46. For example, the MCA, its leadership, and its members have been associated with Rabih Haddad. Rabih Haddad is a 41-year-old native of Lebanon who came legally to the United States and lived until recently in Ann Arbor with his wife and four children. He was an active member of MCA and a volunteer teacher at MCA's Michigan Islamic Academy. In 1992, he co-founded the Global Relief Foundation, a humanitarian organization which the federal government has accused of having provided material support for terrorism. In December 2001, Mr. Haddad was arrested on immigration charges. Though never accused of threatening or harming anyone, Mr. Haddad was denied bond and held in solitary confinement for months with almost no access to his family or the outside world. The INS commenced removal proceedings against him based on visa violations, and the government attempted to close the INS hearings to the press and public. The ACLU, the Detroit Free Press, Representative John Conyers and others successfully sued to open the hearings. Mr. Haddad was ultimately imprisoned for approximately nineteen months, and deported to Lebanon in July 2003. He was never charged with any crime.

47. Some MCA members founded the Free Rabih Haddad Committee in December 2001. The Free Rabih Haddad Committee supported the Haddad family during Mr. Haddad's imprisonment, raised money to assist in his defense, organized public demonstrations in support of Mr. Haddad, and organized a letter-writing campaign. The Free Rabih Haddad Committee continues to educate the public about the government's treatment of Mr. Haddad. The MCA itself also held numerous fundraisers and public rallies to protest Mr. Haddad's detention.

48. Almost all meetings of the Free Rabih Haddad Committee were held at the MCA. During his detention, Mr. Haddad placed weekly telephone calls to the MCA in order to speak with MCA leaders and members.

49. The MCA, its leadership, and its members have also been associated with Dr. Sami Al-Arian. In October 2002, Dr. Sami Al-Arian spoke at the MCA mosque on the "Eroding Status of Our Civil Liberties." Dr. Al-Arian is a Kuwaiti-born former professor at the University of South Florida. He was indicted in the Middle District of Florida in February 2003 for allegedly aiding and abetting terrorism in the occupied West Bank. The federal government has introduced evidence in the case that they obtained through wiretaps authorized under another Patriot Act amendment to FISA. Dr. Al-Arian's daughter, Layla Al-Arian, spoke about her father's case at MCA's mosque in March 2003.

50. Other MCA members and leaders have been individually targeted for investigation by the FBI.

51. For example, MCA member Homam Albaroudi was born in Syria and came to the United States in 1987. He received a Masters in Engineering from Missouri State University and a Ph.D. in Engineering from Oregon State University. He is now a United States citizen. He is married to a United States citizen and has three children, all United States citizens. He works as an engineer for a Fortune 100 company.

52. Mr. Albaroudi has been an active member of MCA since 1999. He was a member of the Michigan Islamic Academy's board of directors for 3 years.

53. Mr. Albaroudi has also been a member of CAIR's Michigan chapter for approximately three years.

54. In 1993, Mr. Albaroudi co-founded the Islamic Assembly of North America ("IANA"), a non-profit organization dedicated to educating the public about Islam. While he was associated with the organization, IANA organized conferences, published religious books, and supplied Qurans to incarcerated Muslims. Mr. Albaroudi served as IANA's Executive Director from the organization's founding in 1996 until 1997, when he stepped down from his position and ended his association with IANA because of personal differences with other IANA leaders. The FBI raided IANA's offices in February 2003, seizing computers and taking photographs of books. The computers contained information about Mr. Albaroudi. FBI agents also questioned IANA associates and ex-employees about Mr. Albaroudi, notwithstanding that his association with IANA ended in 1997.

55. Mr. Albaroudi was also a founder of the Free Rabih Haddad Committee. Mr. Albaroudi convened the initial meeting of the Committee on the premises of the MCA.

56. Mr. Albaroudi has twice been contacted by the FBI. On the first occasion, which was approximately four years ago, Mr. Albaroudi was on an employment-related consulting assignment in Indiana when the FBI came looking for him at his home in Michigan. When the FBI discovered that Mr. Albaroudi was not at home, they left their cards with Mr. Albaroudi's wife, asking that Mr. Albaroudi contact them when he returned. Mr. Albaroudi did so. The FBI did not pursue efforts to speak with Mr. Albaroudi after he informed them that he did not feel comfortable speaking with them without an attorney present.

57. The FBI contacted Mr. Albaroudi again in or about March 2003. On this occasion, the FBI agents who contacted him said that they had not singled him out but rather were interviewing many people in the area to find out whether anyone had learned of conspiracies against the United States. Mr. Albaroudi explained to the FBI that he would have contacted them of his own accord if he had learned of conspiracies against the United States. The FBI then asked Mr. Albaroudi about another co-founder of IANA, who had recently been arrested for an overdraft check and then detained on immigration charges. The FBI did not pursue efforts to speak with Mr. Albaroudi after he informed them that he did not feel comfortable speaking with them without an attorney present.

58. Mr. Albaroudi reasonably believes that, because of his religion, his ethnicity, his place of birth, his earlier leadership role in IANA, his leadership role in the Free Rabi'h Haddad Committee, and his membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain his records and personal belongings.

59. MCA member Kristine Abouzahr was born in Lansing, Michigan in 1958. She is married and has five children, the eldest of whom is 21 and the youngest 9. Mrs. Abouzahr received a B.S. from Oklahoma State University in 1978 and an M.A. from Virginia Polytechnic Institute and State University in 1980. She moved to Michigan in 1986.

60. Mrs. Abouzahr has been a member of the MCA since 1986.

61. Mrs. Abouzahr taught at the Michigan Islamic Academy from 1990-1994, from 1995-1997, from 1999-2001, and during this past academic year. Mrs. Abouzahr's youngest daughter is currently a student at the Michigan Islamic Academy.

62. Mrs. Abouzahr serves on MCA's Outreach Committee, whose mandate is to educate Americans about Islam. As a member of the Outreach Committee, she has visited numerous local schools and community organizations to give presentations about Islam. Mrs. Abouzahr also serves informally as an advisor to Michigan Islamic Academy's new immigrant students and their parents who have questions about adjusting to life in the United States.

63. Mrs. Abouzahr is an active member of the Ann Arbor Area Committee for Peace (AAACP). As a member of that organization, Mrs. Abouzahr attended demonstrations against the Gulf War, against the Patriot Act, against the FBI's "voluntary" interview program, and in favor of a just peace between Israel and Palestine. Mrs. Abouzahr has also spoken publicly at demonstrations sponsored by AAACP and MCA, including at demonstrations in support of Rabih Haddad.

64. Mrs. Abouzahr is also an active member of the Free Rabih Haddad Committee. As one of the Committee's two Media Coordinators, she drafts press releases, speaks to the media, and organizes public demonstrations. She has also spoken publicly in support of Mr. Haddad. For example, in February 2002, after she had traveled to Washington, D.C., with Mr. Haddad's wife, she spoke at an informational forum organized and co-sponsored by the AAACP and the Free Rabih Haddad Committee to inform the local community about Haddad's case.

65. The Free Rabih Haddad Committee's post office box is registered in Mrs. Abouzahr's name.

66. Mrs. Abouzahr reasonably believes that, because of her religion, her leadership role in the Free Rabih Haddad Committee, her membership in AAACP, and

her membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain her records and personal belongings.

67. MCA member Nazih Hassan was born in Lebanon in 1969. He emigrated to Canada in 1988 and became a Canadian citizen in 1993. Mr. Hassan received his B.Esc. from the University of Western Ontario in 1994.

68. Mr. Hassan came to the United States in 1994 to study at Eastern Michigan University. He received his M.S. in Computer Information Systems from that institution in 1997.

69. Mr. Hassan became a legal permanent resident in 2001. He is married and has three children, two of whom are United States citizens. Mr. Hassan now works as a technology consultant and resides in Ypsilanti, Michigan.

70. Mr. Hassan has been a member of the MCA since 1994. Since January 2002, he has served as MCA's President. At various times since 1995, he also served as Editor of MCA's newsletter, as MCA's Secretary, and as MCA's Vice President.

71. Mr. Hassan was a founder of the Free Rabih Haddad Committee. As one of the Committee's two Media Coordinators, he drafts press releases, speaks to the media, and organizes public demonstrations.

72. Mr. Hassan reasonably believes that, because of his religion, his ethnicity, his place of birth, his leadership role in the Free Rabih Haddad Committee, and his membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain his records and personal belongings.

73. MCA also reasonably believes that it could be served with a Section 215 order. It then would have no ability to challenge the order before compromising the

privacy and free speech rights of its members. MCA maintains various records pertaining to its members, including records of members' names, telephone numbers, e-mail, home and business addresses, and citizenship status and national origin. MCA keeps records relating to members' marriages and divorces, and relating to members' family problems that MCA's Imam and Social Committee help resolve. MCA also keeps records documenting the use of zakat (members' charitable donations). The Michigan Islamic Academy also maintains a variety of educational and counseling records about its students. Finally, MCA has a variety of religious documents associated with the mosque and the Michigan Islamic Academy.

74. MCA has a policy of strictly maintaining the privacy of its records and routinely assures its members that any information they provide to MCA will be kept confidential. MCA's members rely on MCA's assurances that their records will be kept confidential.

75. Section 215 compromises MCA's ability to maintain the confidentiality of records pertaining to its members and students, and to protect individual members and students from harassment, threats, and violence. MCA has been the target of harassment since September 11th. For example, on some occasions after MCA President Nazih Hassan was quoted in newspaper articles, the MCA received several hate letters. After Mr. Hassan wrote a letter to the Ann Arbor News at the end of March 2003, an unknown individual or group placed hate fliers on cars outside the mosque. Were the confidentiality of MCA's records to be compromised and MCA's membership list to become public knowledge, MCA's individual members would be subjected to verbal harassment, threats, and even violence.

76. MCA's ability to keep its records confidential also allows MCA to protect its members and students from the possibility that the government will target them for their exercise of First Amendment rights, including their rights to free speech, free association, and free exercise of religion.

77. Because of the likelihood that the FBI is using provisions of the Patriot Act to target MCA, its leadership, and its members, some MCA members are afraid to attend mosque, to practice their religion, or to express their opinions about religious and political issues. Several people have told MCA leaders that they do not attend mosque for fear that the FBI is surveilling MCA and intends to investigate those who are associated with the organization.

American-Arab Anti-Discrimination Committee

78. ADC is a non-profit civil rights organization committed to defending the rights and promoting the rich cultural heritage of people of Arab descent. ADC has members and volunteer-based chapters in many states. It is headquartered in Washington, D.C., and has staffed offices in New York City, Detroit, San Diego, and San Francisco.

79. Since the passage of the Patriot Act, ADC has spent a significant amount of time, staff resources, and funds in advocating against the civil rights encroachments authorized by the Act. ADC has co-sponsored congressional briefings in Washington, D.C., and held town hall meetings throughout the country to educate the public about the Act. Most recently, ADC was a major co-sponsor of a national congressional briefing held on Capitol Hill on June 4, 2003. The briefing, which was attended by several prominent senators and representatives, featured testimony from immigrants who had

suffered civil rights violations after September 11th. On June 2, 2003, ADC co-sponsored another congressional staff briefing focusing on the Act and other post-September 11 Department of Justice initiatives. ADC staff members have spoken about the Patriot Act at over 150 conferences, seminars, and university events around the nation. Additionally, ADC's National Conventions for 2002 and 2003 included several panels discussing the Patriot Act and other government programs and policies implemented after the Patriot Act became law. ADC spokespeople, including Communications Director Hussein Ibish, are among the leading advocates in national media against the Patriot Act. Moreover, the ADC Legal Department provides routine assistance to anyone contacting ADC for help concerning law enforcement or other activities related to the Patriot Act. Finally, ADC's Legal Department is an active participant in coalition-based policy advocacy to amend or repeal parts of the Act.

80. ADC monitors the due process and equal protection rights of all Arab-Americans, including those who were detained on by the INS after September 11th and those who have been caught up in terrorism investigations.

81. For example, ADC and its members publicly condemned the use of secret evidence in the detention of Dr. Mazen Al-Najjar, formerly a University of South Florida professor. Though incarcerated for over three years, Dr. Al-Najjar was never charged with any criminal offense. He was ultimately deported for visa violations.

82. ADC and its members have also made public statements of concern about due process issues in the case of Rabi Haddad, a community leader in Ann Arbor, Michigan who was detained by the INS in December 2001, imprisoned for approximately

nineteen months, and ultimately deported in July 2003 without having been charged with any crime.

83. Because of the relationship between ADC, its members, and persons questioned, detained, or deported since September 11th, ADC reasonably believes that the FBI has used or is currently using Section 215 to obtain records and personal belongings about it and its members.

84. ADC also reasonably believes that it could be served with a Section 215 order. ADC would then would have no ability to challenge the order before compromising the privacy rights of its members. ADC maintains a variety of records about members, including their names and names of family members, home and business mailing addresses, phone numbers, email addresses, credit card information, and checking account information. ADC has a policy of maintaining the confidentiality of its members and their private information. ADC does not disclose membership numbers or any other information about members.

85. Section 215 compromises ADC's ability to maintain the confidentiality of records pertaining to its members, and to protect members from harassment, threats, and violence. ADC has documented a substantial increase in hate crimes, discrimination, and harassment against Arab-Americans since the September 11th attacks. Many of these incidents are described in the ADC publication, "Report on Hate Crimes and Discrimination Against Arab Americans; The Post-September 11 Backlash." Over 700 violent incidents occurred in the first nine weeks following the attack, including several murders. In the first year after the attacks, ADC documented over 80 cases in which airlines had discriminated against passengers who were perceived to be Arab. There

were also over 800 cases of employment discrimination against Arab-Americans, an approximately four-fold increase over previous annual rates, and numerous instances of denial of service, discriminatory service and housing discrimination. These numbers remain significantly above pre-September 11th levels today. Were the confidentiality of ADC's records to be compromised or ADC's full membership list to become public knowledge, ADC's members could risk harassment, threats, and even violence.

Arab Community Center for Economic and Social Services

86. ACCESS is a human services organization committed to the development of the Arab-American community in the United States. Its staff and volunteers serve low-income families, help newly arrived immigrants adapt to life in the United States, and educate Americans about Arab culture. ACCESS provides a wide range of social, mental health, educational, artistic, employment, legal and medical services. ACCESS has more than 2500 members and approximately 150 full-time staff.

87. ACCESS provides over seventy different programs to more than a hundred thousand people of all ethnic and religious backgrounds. In the last fiscal year, ACCESS provided more than 57,290 services in the area of social and legal services, more than 12,600 counseling and psychiatric services, more than 60,300 in health and health education services, and more than 55,600 employment and vocational services. ACCESS also provided more than 256,590 hours of educational and recreational services to youths and their parents, and sponsored cultural events and activities attended by many thousands of people.

88. For example, ACCESS runs a Community Health and Resources Center that offers a wide range of medical, public health, mental health and family counseling

services and programs. Its division of Psychosocial Rehabilitation for Survivors of Torture and Refugee Family Strengthening provides mental health services to torture victims and refugees. ACCESS also provides specialized services to victims of domestic violence, administers a breast and cervical cancer control program, and provides HIV/AIDS and STD education, counseling and testing. The Center's research division has twice sponsored a National Conference on Health Issues in the Arab Community.

89. ACCESS's Department of Social Services offers emergency food assistance, immigration services, and homelessness prevention programs. Its Department of Employment and Training offers a variety of job training programs, language instruction, and family acculturation services to help immigrants integrate into their new society. The Youth and Education Department provides after school homework assistance to students, special programs for at-risk youth, and recreation programs and teen dialogue opportunities for young people.

90. Because of the relationship between ACCESS, its members and clients, and persons questioned, detained, or deported since September 11th, ACCESS reasonably believes that the FBI has used or is currently using Section 215 to obtain records or other personal belongings about it and its members and clients.

91. Some of ACCESS's members and clients have been individually targeted for investigation by the FBI.

92. For example, ACCESS member Ahmad Ali Ghosn was born in Lebanon in 1965. He has been a legal permanent resident of the United States since 1993. Mr. Ghosn's application for naturalization has been pending for over seven years. Mr. Ghosn first submitted his application in June 1996. The INS later informed Mr. Ghosn that it

had lost the application and advised him to submit two duplicate applications. Mr. Ghosn did so. He received an acknowledgement notice from the INS in January 1998 – over five years ago. Since January 1998, the INS has required Mr. Ghosn to be fingerprinted on multiple occasions but it has never sought to schedule a naturalization interview.

93. The INS most recently required Mr. Ghosn to be fingerprinted in February 2002. When Mr. Ghosn appeared as he had been asked to, he was greeted not only by an INS criminal investigator but also by two FBI agents, who questioned him for over two hours about his associations with various individuals and charitable organizations in Lebanon. The FBI agents informed Mr. Ghosn that he could be naturalized if he cooperated with them, but that if he did not, his children would be seized by the government and placed in foster care. Mr. Ghosn answered the FBI's questions to the best of his ability but refused their request that he become an FBI or INS spy. He was not advised of his right to counsel.

94. Because of the FBI's actions, Mr. Ghosn reasonably believes that the FBI has used or is currently using Section 215 to obtain his records or other personal belongings.

95. ACCESS also reasonably believes that it could be served with a Section 215 order. It would then have no ability to challenge the order before compromising the privacy rights of its members and clients. ACCESS maintains a wide range of highly personal, sensitive records relating to the services it offers to clients. For example, the Community Health and Research Center maintains medical records for torture victims and refugees, and for breast cancer, mental health, and HIV/AIDS patients. It also

maintains files on domestic violence victims and family counseling clients. ACCESS routinely assures its clients that the information they provide will be kept confidential.

Bridge Refugee & Sponsorship Services

96. Bridge is an ecumenical, non-profit organization that helps refugees and asylum-seekers become and stay self-sufficient.

97. Bridge is affiliated with Church World Service ("CWS"), which is the relief, development, and refugee assistance ministry of 36 Protestant, Orthodox, and Anglican denominations in the United States, and with Episcopal Migration Ministries ("EMM"), which is the arm of the Episcopal Church that advocates for the protection of the refugees.

98. Bridge employs eight staff members and has offices in Knoxville, Chattanooga, and Bristol, Tennessee.

99. Bridge generally obtains clients in either of two ways. In some cases, a person residing in the United States asks Bridge to assist a relative whom the United States has granted refugee status but who has not yet arrived in the United States. In these cases (called "family reunification" cases), Bridge begins working with the refugee's family while the refugee is still outside the United States. In other cases, Bridge is assigned refugees' files by affiliate organizations such as CWS and EMM. These cases (called "free" cases) usually involve refugees who do not have family in the United States.

100. Historically, Bridge has served approximately 200 new refugees and asylum seekers in a year. Bridge's current caseload, which includes refugees who arrived in the United States over the last five years, includes approximately 500 files.

101. Bridge ordinarily serves its clients through individual sponsors, whom Bridge recruits from local churches, mosques, and synagogues.

102. Sponsors sign confidentiality agreements. Bridge staff explain and review the confidentiality agreement in sponsor training sessions.

103. Bridge provides its clients with a broad spectrum of resettlement services. For example, Bridge staff and sponsors ensure that new refugees have accommodations, furniture, clothing, and food; accompany new refugees to the Department of Health for medical examinations and immunizations; provide English language tutors to refugees who require them; ensure that refugee children enroll in school; provide cultural counseling to educate new refugees about American customs; assist new refugees in finding employment as quickly as possible; assist new refugees in complying with immigration requirements; assist refugees in applying for permanent residence and citizenship; direct refugees to social services provided by other organizations or by the federal and state governments; and counsel refugees about personal problems, including substance abuse, sexual abuse, discrimination at work or school, domestic violence, family planning, and divorce.

104. Bridge maintains various records pertaining to its clients, including records of clients' names, telephone numbers, and residential addresses. Bridge also keeps records of its clients' dates of arrival in the United States.

105. In many cases, Bridge's files also include case notes taken by Bridge staff. Case notes may document medical conditions from which the client has suffered in the past or that the client suffers currently. Case notes may also document the nature of the persecution that the client faced in her home country.

106. In some cases, clients consult Bridge staff about personal problems, including substance abuse, sexual abuse, discrimination at work or school, domestic violence, family planning, and divorce. In one case, for example, Bridge counseled a client about a venereal disease that she had acquired as a result of rape by a soldier. In another case, Bridge counseled an elderly client who was being mistreated by his daughters. Bridge's case notes include documentation of conversations relating to these and similarly intimate, personal problems.

107. In many cases, Bridge's refugee clients can obtain the assistance they need only from Bridge. There is no other resettlement services organization in East Tennessee whose staff have the relevant language and professional skills. When Bridge's clients decide that they cannot afford to entrust their personal information to Bridge, those clients generally do not obtain the help that they need from anywhere. They simply deal with their problems – including serious medical and personal problems – on their own.

108. Bridge is concerned that Section 215 compromises its ability to maintain the confidentiality of its clients' records. Bridge regularly assures its clients that the information they provide will be kept confidential, and explains that, under state law, the confidentiality of the information that clients provide is protected by a social worker privilege. Bridge provides its clients with a confidentiality agreement that assures clients that Bridge will disclose their records only "to facilitate the continuation of proper medical treatment and social services."

109. Bridge reasonably believes that it could be served with a Section 215 order. Bridge would then would have no ability to challenge the order before compromising the privacy rights of its members.

110. The FBI has approached Bridge for information about its clients on at least two occasions. In early November 2002, the FBI approached Bridge to ask it to disclose all records relating to its Iraqi-born clients. Bridge declined to disclose the records because the records included sensitive, personal information, including medical information.

111. On November 12, 2002, Bridge was served with a Subpoena To Testify Before Grand Jury, ordering the production of "Any and all records of Bridge . . . relating to any and all Iraqi-born people who have been assisted by Bridge Refugee and Sponsorship Services, Inc., including records that provide the name, address, telephone number, employer, and personal circumstances of such persons." Bridge moved to quash the subpoena but withdrew its motion when the FBI agreed not to seek more information than Bridge's clients would already have provided to the INS. The FBI made clear, however, that it might eventually demand more information. The FBI did not indicate what form such a demand might take.

112. Bridge client Muwafa Albaraqi was born in 1968 in Najaf, Iraq, where he lived until 1991. In 1991, at the encouragement of the United States, Mr. Albaraqi participated in an uprising against the government of Saddam Hussein. Although the uprising was successful in Najaf, American support did not materialize and ultimately the city fell again to the Iraqi Republican Guard. Those who had participated in the uprising were labeled traitors and were tortured, imprisoned, or killed. Mr. Albaraqi fled to Saudi Arabia.

113. Mr. Albaraqi lived in a United Nations-administered refugee camp in Saudi Arabia from March 1991 to September 1994. He applied for political asylum in the United States while living at the camp.

114. Mr. Albaraqi came to the United States in September 1994. His file, which was initially assigned to another refugee organization, was transferred to Bridge when Mr. Albaraqi decided that he would reside in Tennessee, where he had friends.

115. Bridge assisted Mr. Albaraqi in adjusting to life in Tennessee. For example, Bridge showed Mr. Albaraqi around Knoxville, pointing out where he could buy groceries and clothing, and showed him how to use the bus system. Bridge helped Mr. Albaraqi find a place to live, paid his first month's rent and utilities, and bought him groceries for his first week in the country. Bridge also helped Mr. Albaraqi apply for federal assistance, including food stamps and social security. Bridge accompanied Mr. Albaraqi to the Department of Health, where Mr. Albaraqi was given a medical examination and immunizations. Bridge also helped Mr. Albaraqi with his application for permanent residence and, eventually, his application for citizenship.

116. Mr. Albaraqi became a United States citizen in 1999. Mr. Albaraqi now works as a check-out clerk at a grocery store in Knoxville, Tennessee. He is also a part-time student in electrical engineering at the University of Tennessee.

117. The FBI came to Mr. Albaraqi's workplace in January 2003, stating that they wanted to talk to him. Mr. Albaraqi was not told that the interview was optional or voluntary or that he had a right to contact an attorney and have an attorney present at the interview.

118. During the interview, the FBI asked, among other questions, whether anyone associated with the Iraqi government had asked him to engage in terrorism against American targets; what he would do if an Iraqi agent asked him to engage in terrorism; and whether he might act differently if the Iraqi agent cut off his brother's finger and sent it to him in the mail.

119. Mr. Albaraqi would not have sought Bridge's assistance for sensitive, personal matters had he thought that the FBI could easily access Bridge's records under Section 215. Based on his own experience as a refugee, he believes that other refugees will be less likely to seek help from Bridge because the FBI can obtain their sensitive, personal records even when they have done nothing wrong.

Council on American-Islamic Relations

120. CAIR is a non-profit, grassroots organization dedicated to enhancing the public's understanding of Islam and Muslims. CAIR is the largest Islamic civil liberties organization in the United States. CAIR's national office in Washington, D.C., has a permanent staff of about 25 people. Approximately the same number of people are employed by CAIR's state and local chapters.

121. Since the passage of the Patriot Act, CAIR has spent a significant amount of time, staff resources, and funds in advocating against the civil rights encroachments authorized by the Act. CAIR hosts an annual conference each March. At both the 2002 and 2003 conferences, multiple speakers explained the Patriot Act and discussed its import for Muslims in the United States. CAIR hosts an annual dinner each October. At both the 2001 and 2002 dinners, speakers explained the Patriot Act and discussed its import for Muslims in the United States. CAIR regularly distributes e-mail "Action

Alerts” to members and others who have subscribed to CAIR’s Action Alert list. Since the Patriot Act became law, CAIR has distributed numerous Action Alerts related to the Patriot Act. CAIR has also issued numerous news releases related to the Patriot Act.

122. CAIR monitors the due process and equal protection rights of all Muslims living in the United States, including those detained on immigration charges after September 11th and those caught up in terrorism investigations. In 2002, CAIR issued a 54-page “Civil Rights Report” that, among other things, examined the impact that “anti-terrorism” policies, including the Patriot Act, had had on the civil liberties of American Muslims. CAIR issued a similar Civil Rights Report in 2001 and issued a new Civil Rights Report in July 2003.

123. Because of the relationship between CAIR, its members, and persons questioned, detained, or deported since September 11th, CAIR reasonably believes that the FBI is currently using Section 215 to obtain records and personal belongings of CAIR and its members.

124. For example, CAIR member Magda Bayoumi was born in Cairo, Egypt, in 1956. She came to the United States in 1977 and became a United States citizen in 1988. Mrs. Bayoumi has been a member of CAIR for approximately four years.

125. Mrs. Bayoumi is married and has three children, of whom the youngest is 10 and the eldest 17. Mrs. Bayoumi's husband was also born in Cairo, Egypt. He became a United States citizen in 1991. All of Mrs. Bayoumi's children are United States citizens. Mrs. Bayoumi and her family live in Syracuse, New York.

126. Mrs. Bayoumi works as a volunteer for several community organizations. She currently chairs the board of the Parents Advisory Group for the Special-Education

Director of the Syracuse School District. She serves as a board member of the Central New York Parent's Coalition for Children With Special Needs. She co-founded and serves on the board of the of Autism Support Group. She founded and serves on the board of the Ed Smith School's Support Group for Children With Special Needs.

127. Mrs. Bayoumi and her husband co-founded and serve on the board of the Central New York Chapter of the American Muslim Council, an organization that was established in 1990 to increase the effective participation of American Muslims in the political process.

128. Two FBI agents came to Mrs. Bayoumi's home on February 26, 2003. They first informed Mrs. Bayoumi that they wanted to question her husband. When Ms. Bayoumi told the agents that her husband was not at home, however, they began to question her instead.

129. The FBI's questioning focused on a donation that Mrs. Bayoumi and her husband had made to a charity called Help the Needy. Mrs. Bayoumi and her husband had donated several hundred dollars to the organization the previous year.

130. The agents asked Mrs. Bayoumi how much money she and her husband had contributed to the charity, whether she had attended a dinner that Help the Needy had recently hosted, whether she knew what the donation was being used for, and whether she would be upset if the money had been used to build a mosque. Mrs. Bayoumi told the FBI that she and her husband had donated a few hundred dollars to the charity in each of the previous few years, had attended the recent dinner, and had assumed that the donation would be used to provide food and medicine for needy people in Iraq.

131. The FBI did not inform Mrs. Bayoumi how they had learned that she and her husband had made a donation to Help the Needy.

132. On the same day that the FBI questioned Mrs. Bayoumi, the Department of Justice announced that a federal grand jury in Syracuse, New York, had returned an indictment charging Help the Needy and four individuals associated with it of transferring funds to persons in Iraq without having obtained the proper license. While Help the Needy was not accused of having providing anything other than humanitarian aid to people living in Iraq, the Justice Department's press release accused Help the Needy of attempting to undermine the President's efforts "to end Saddam Hussein's tyranny and support for terror."

133. Mrs. Bayoumi reasonably believes that because of her religion, her ethnicity, and her earlier support for Help the Needy, the FBI has used and is currently using Section 215 to obtain her records and other personal belongings.

134. CAIR also reasonably believes that it could be served with a Section 215 order. CAIR would then would have no ability to challenge the order before compromising the privacy rights of its members. CAIR maintains a variety of records about members, including their names, home and business mailing addresses, phone numbers, email addresses, credit card information, and checking account information. CAIR has a policy of maintaining the confidentiality of its members and their private information. CAIR does not disclose membership numbers or any other information about individual members.

135. Section 215 compromises CAIR's ability to maintain the confidentiality of records pertaining to its members, and to protect members from harassment, threats, and

violence. CAIR has documented a substantial increase in hate crimes, discrimination, and harassment against Muslim and Arab-Americans since the September 11th attacks. Many of these incidents are described in CAIR's 2001, 2002, and 2003 Civil Rights Reports. Were the confidentiality of CAIR's records to be compromised and CAIR's membership list to become public knowledge, CAIR members could risk harassment, threats, and even violence.

Islamic Center of Portland, Masjed As-Saber

136. The Islamic Center of Portland, Masjed As-Saber ("ICPMA"), is a non-profit organization that owns and administers a mosque known as Masjed As-Saber and an Islamic school known as the Islamic School of Portland. Approximately 450 people attend services at the mosque each Friday; as many as 3500 attend services on religious holidays. ICPMA employs approximately 16 people. Approximately 60 students are enrolled at the school.

137. Because of the relationship between ICPMA, its community members and leaders, and persons and organizations investigated, questioned, detained, or arrested since September 11th, ICPMA reasonably believes that the FBI has used or is currently using Section 215 to obtain records and personal belongings pertaining to it and its community members and students.

138. Some ICPMA community members have been individually targeted for investigation by the FBI.

139. In October, 2002, a federal grand jury in the District of Oregon indicted six individuals and charged them with various counts of conspiracy to wage war against the United States and to provide material support to Al Qaeda; a seventh individual was

indicted on similar charges in April 2003. A trial is currently scheduled for January 2004 in this case, which is known as the "Portland 7" case. Some of the defendants, Jeffrey Leon Battle, Patrice Lumumba Ford, and Habis Abdulla al Saoub, attended the ICPMA. In an affidavit submitted in support of the indictment of the defendants, Police Officer Thomas W. McCartney stated that a wired informant recorded conversations inside the Islamic Center of Portland, Masjed As-Saber, on June 6, 2002. The electronic surveillance was authorized under another Patriot Act amendment to FISA. The affidavit also states that the government obtained a number of records relating to the investigation. The affidavit does not state the legal authority utilized in obtaining these records. The government has stated publicly that the investigation into the alleged conspiracies is ongoing.

140. The FBI has also sought records from ICPMA. In March 2003, the ICPMA was served with a subpoena seeking financial records related to the defendants and their spouses in the Portland 7 case. ICPMA retained lawyers who moved to quash the subpoena because of the impact on the privacy rights of ICPMA's constituents, but was ultimately required to disclose the records. Some of ICPMA's constituents are now afraid to donate to ICPMA because they fear their donations will provoke FBI investigation and harassment. The FBI has also served subpoenas to over 25 people in the Portland area, some of whom attend ICPMA and other local mosques. The FBI has interviewed some ICPMA community members and has asked questions about other worshipers and their political and religious views.

141. In addition, some of ICPMA's leaders appear to be under investigation by the FBI but have not been charged with any crime.

142. For example, ICPMA president Alaa Abunijem was born in Saudi Arabia and came to the United States in 1989. He became a U.S. citizen in 1996. Mr. Abunijem is married to a U.S. citizen and has four children. He holds a B.S. degree in Electrical Engineering and an M.S. in Engineering and Technology Management. He currently works as an engineer for a Fortune 100 company, and has lived in Portland, Oregon, since 1999.

143. On December 17, 2002, Mr. Abunijem was stopped at the Seattle airport by U.S. Customs and questioned by both U.S. customs and FBI officials regarding the purpose of his trip to Saudi Arabia. The officials searched his documents, business cards, and credit cards for thirty minutes before returning them to him. On his return from Saudi Arabia on January 9, 2003, his luggage and documents were searched for over an hour and a half, and he was questioned by officials about his trip.

144. On February 26, 2003, an FBI agent called Mr. Abunijem at his work place and questioned him about a donation he had made to a charity called Help the Needy. Mr. Abunijem had made donations of several hundred dollars to the organization over the past few years. The FBI did not inform Mr. Abunijem how they had learned that he made a donation to Help the Needy. Mr. Abunijem told the FBI agent that he did not feel comfortable talking to the FBI without a lawyer.

145. On the same day that the FBI questioned Mr. Abunijem, the Department of Justice announced that a federal grand jury in Syracuse, New York, had returned an indictment charging Help the Needy and four individuals associated with it of transferring funds to persons in Iraq without having obtained the proper license. While Help the Needy was not accused of having providing anything other than humanitarian

aid to people living in Iraq, the Justice Department's press release accused Help the Needy of attempting to undermine the President's efforts "to end Saddam Hussein's tyranny and support for terror."

146. Since 1999, Mr. Abunijem has served as a board member of the Islamic Assembly of North America ("IANA"), a non-profit organization dedicated to educating the public about Islam. IANA organizes conferences, publishes religious books, and supplies Qurans to incarcerated Muslims. The FBI raided IANA's offices in Michigan in or about February 2003, seizing computers and taking photographs of books. The computers contained information about Mr. Abunijem. The government has not charged IANA with any crime, but has arrested one of the organization's former presidents, Bassem K. Khafagi, on federal bank fraud charges. Assistant U.S. Attorney Terry Derden of Boise, Idaho has stated publicly that "the investigation could expand to other directors and Islamic Assembly employees."

147. Mr. Abunijem has not been charged with any crime and strongly maintains his innocence.

148. Mr. Abunijem reasonably believes that because of his religion, his ethnicity, his place of birth, his leadership role in ICPMA and IANA, and his donations to Help the Needy, the FBI is currently using Section 215 to obtain his records and personal belongings.

149. ICPMA reasonably believes that it could be served with a Section 215 order. It would then have no ability to challenge the order before compromising the privacy rights of its members. ICPMA maintains a variety of records about community members, including their names and the names of family members, home and business

mailing addresses, phone numbers, email addresses, credit card information, and checking account information. ICPMA also retains records of services it provides to community members, including Islamic marriage contracts, and records of divorce proceedings and financial assistance given to needy families. The Islamic School of Portland retains health, financial and educational records pertaining to all of its students and staff. ICPMA has a policy of maintaining the confidentiality of all records pertaining to its community members, staff and students.

150. Section 215 compromises ICPMA's ability to maintain the confidentiality of its records, and to protect community members and students from harassment, threats, and violence. Since the September 11th attacks, ICPMA community members and other Arab-Americans have repeatedly been the target of harassment. Were the confidentiality of ICPMA's records to be compromised and ICPMA's community list or other records to become public knowledge, ICPMA's community members and students could risk verbal harassment, threats, and even violence.

151. ICPMA's ability to keep its records confidential also allows ICPMA to protect its community members from the possibility that the government will target them for their association with ICPMA, including their rights to free speech, free association, and free exercise of religion.

152. Because ICPMA community members believe that the FBI is currently using provisions of the Patriot Act to target ICPMA, and because the FBI has recorded conversations and services inside the mosque and sought records from ICPMA, many ICPMA community members are afraid to attend mosque, practice their religion, or express their opinions about religious and political issues.

CAUSES OF ACTION

153. Section 215 violates the Fourth Amendment by authorizing the FBI to execute searches without criminal or foreign intelligence probable cause.

154. Section 215 violates the Fourth Amendment by authorizing the FBI to execute searches without providing targeted individuals with notice or an opportunity to be heard.

155. Section 215 violates the Fifth Amendment by authorizing the FBI to deprive individuals of property without due process.

156. Section 215 violates the First Amendment by categorically and permanently prohibiting any person from disclosing to any other person that the FBI has sought records or personal belongings.

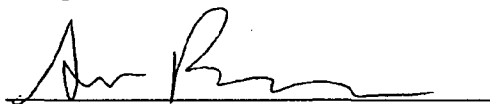
157. Section 215 violates the First Amendment by authorizing the FBI to investigate individuals based on their exercise of First Amendment rights, including the rights of free expression, free association, and free exercise of religion.

PRAYER FOR RELIEF

WHEREFORE Plaintiff respectfully requests that the Court:

1. Declare that Section 215 is unconstitutional under the First, Fourth, and Fifth Amendments.
2. Permanently enjoin Defendants from using Section 215.
3. Award Plaintiff fees and costs pursuant to 28 U.S.C. § 2412.
4. Grant such other and further relief as the Court deems just and proper.

Respectfully submitted,



ANN BEESON

JAMEEL JAFFER

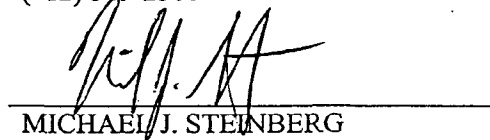
National Legal Department

American Civil Liberties Union
Foundation

125 Broad Street, 18th Floor

New York, NY 10004-2400

(212) 549-2500



MICHAEL J. STEINBERG

NOEL SALEH

KARY L. MOSS

American Civil Liberties Union Fund
of Michigan

60 West Hancock

Detroit, MI 48201-1343

(313) 578-6800

Dated: July 30, 2003

Patriot Act: Section 215 - Library/Bookstore Records

Issue: Does Section 215 of the Patriot Act represent a threat to the privacy of those who patronize libraries and bookstores?

Response:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-cv-0845

- Section 215 amended the business records authority found in the Foreign Intelligence Surveillance Act (FISA). Under the former language, the FISA Court could issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power.
- The Patriot Act changed the standard to **simple relevance** and authorizes compelled production in relation to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution. The Patriot Act also broadens the categories of items that can be obtained; the authority can now be used for "the production of any tangible thing."
- Section 215 is not a radical expansion of federal investigative authority. Federal grand juries have long had power to issue subpoenas to all types of organizations, including libraries and bookstores, without a probable cause requirement. Several high-profile investigations (Unabomber, NRO spy Brian Regan) involved subpoenas to and/or surveillance in public libraries.
- When we are conducting a covert investigation of a suspected spy or terrorist, it is vitally important that he or she not learn of our request for records. The non-disclosure provision in 215 is also not a radical innovation; similar provisions exist preventing financial institutions (12 USC § 3414) and communications service providers (18 USC § 2709) from disclosing that the FBI obtained information pertaining to customer records.
- The FBI conducted an informal survey of field offices that revealed fewer than 50 contacts with libraries after 9/11. All of those contacts were based on specific leads or subjects. The vast majority of the contacts were based on voluntary reports by library personnel of suspicious behavior by patrons.
- It is important to note that the FBI does not open investigations on how persons exercise their First Amendment rights or on the lawful exercise of any other rights secured by the Constitution or federal statute. FBI counterterrorism investigations are opened, pursuant to the Attorney General Guidelines, based on information indicating terrorist activity.

Certification must state:

- ① Certifying official deems information sought to be foreign intelligence information
- ② That a significant purpose of surveillance is to obtain foreign intelligence information

Foreign intelligence information means

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-cv-0845

1. information that relates to, and if concerning a US person is necessary to, the ability of the US to protect against —

- A. actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
- B. sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- C. clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

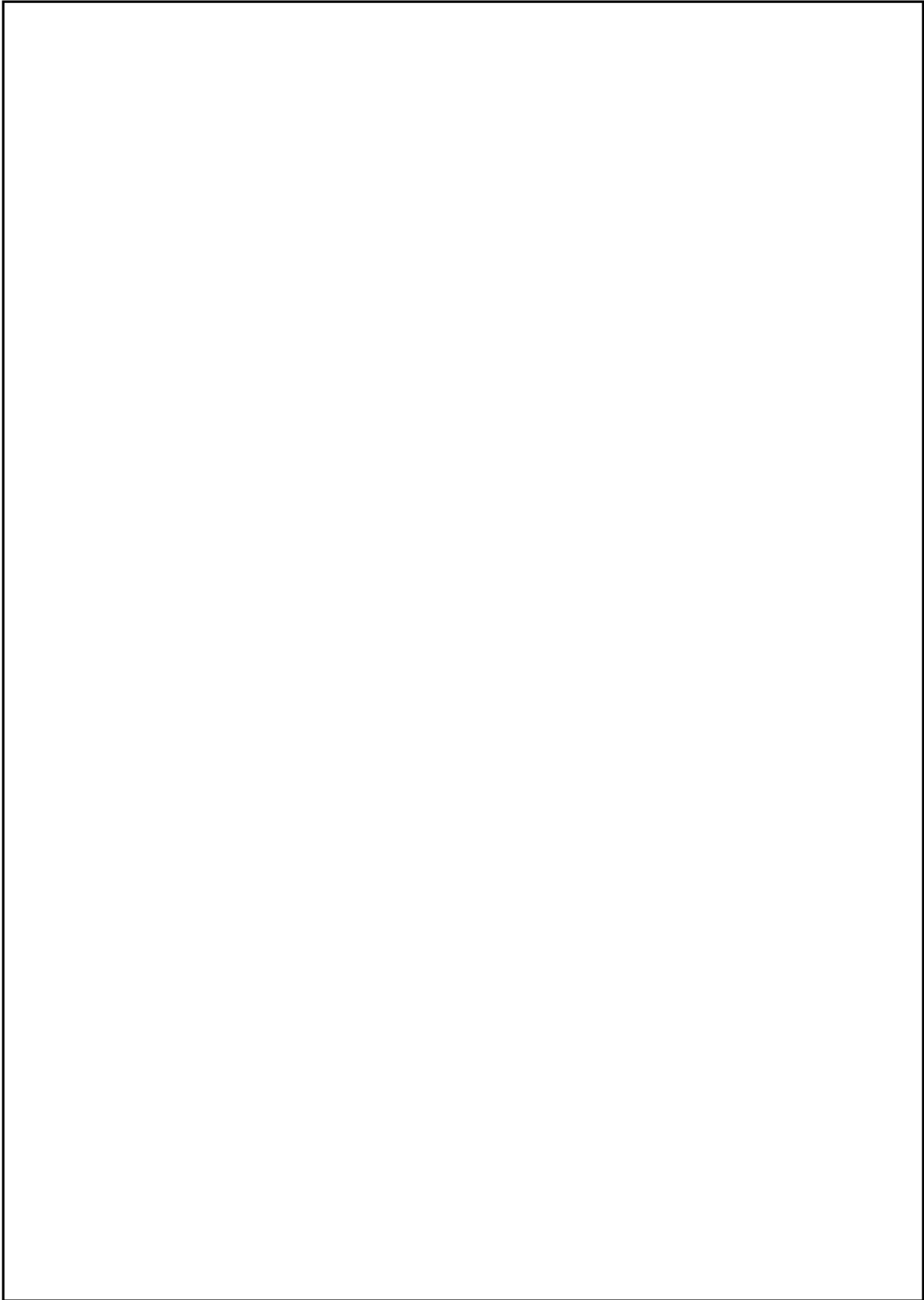
or

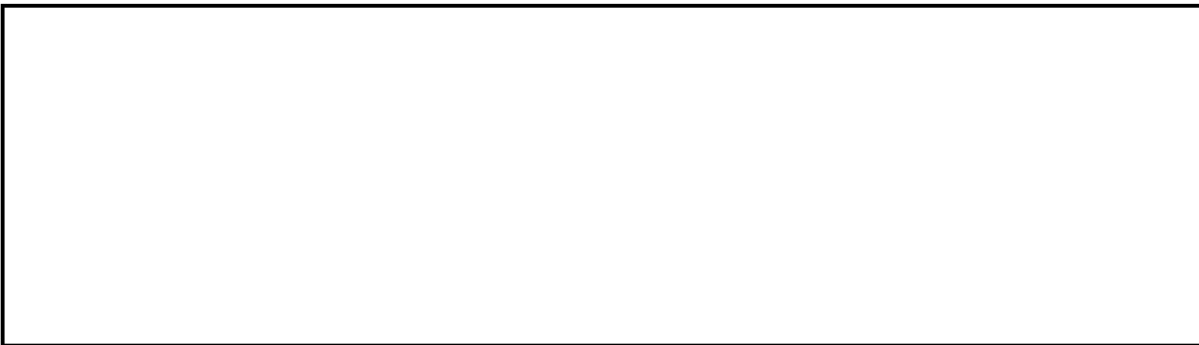
2. information with respect to a foreign power or foreign territory that relates to, and if concerning a US person is necessary to —

- A. the national defense or the security of the U.S. or
- B. the conduct of the foreign affairs of the U.S.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-CV-0845

b5





CRS Report for Congress

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework

Updated April 29, 2002

Elizabeth B. Bazan
Legislative Attorney
American Law Division

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-16-2005 BY 65179/DMH/LP/RW 05-cv-0845



Prepared for Members and
Committees of Congress



The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework

Summary

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, provides a statutory framework for electronic surveillance in the context of foreign intelligence gathering. In so doing, the Congress sought to strike a delicate balance between national security interests and personal privacy rights. Subsequent legislation expanded federal laws dealing with foreign intelligence gathering to address physical searches, pen registers and trap and trace devices, and access to certain business records. P.L. 107-56 made significant changes to some of these provisions. This report will examine the detailed statutory structure provided by the Foreign Intelligence Surveillance Act, as amended (FISA), and related provisions of E.O. 12333. It is current through the changes to FISA in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56, which was signed into law by President George W. Bush on October 26, 2001, and the amendments included in the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, which was signed into law by the President on December 28, 2001.

Contents

Introduction	1
Background	1
Executive Order 12333	4
The Foreign Intelligence Surveillance Act	6
The Statutory Framework	6
Electronic surveillance under FISA	6
Physical searches for foreign intelligence gathering purposes	26
Pen registers or trap and trace devices used for foreign intelligence gathering purposes	38
Access to certain business records for foreign intelligence purposes	44
New Private Right of Action	47
USA PATRIOT Act Sunset Provision	48
Conclusion	48

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework

Introduction

On October 26, 2001, President George W. Bush signed P.L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act or the USA PATRIOT Act. Among its provisions are a number which impacted or amended the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* (FISA). For example, the new law expanded the number of United States district court judges on the Foreign Intelligence Surveillance Court and provided for roving or multipoint electronic surveillance authority under FISA. It also amended FISA provisions with respect to pen registers and trap and trace devices and access to business records. In addition, FISA, as amended, substantially expanded the reach of the business records provisions. The amended language changed the certification demanded of a federal officer applying for a FISA order for electronic surveillance from requiring a certification that *the* purpose of the surveillance is to obtain foreign intelligence information to requiring certification that *a significant purpose* of the surveillance is to obtain foreign intelligence information. FISA, as amended, also affords persons aggrieved by inappropriate use or disclosure of information gathered in or derived from a FISA surveillance, physical search or use of a pen register or trap and trace device a private right of action. Of the amendments made by the USA PATRIOT Act, all but the section which increased the number of judges on the Foreign Intelligence Surveillance Court will sunset on December 31, 2005.

This report will provide background on the Foreign Intelligence Surveillance Act, and discuss its statutory framework, as modified by P.L. 107-56. Where applicable, this report will also note the amendments to FISA reflected in P.L. 107-108 (H.R. 2883), the Intelligence Authorization Act for Fiscal Year 2002, which was signed into law by the President on December 28, 2001.

Background

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests.¹ The stage was set for legislation to address these

¹The Fourth Amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no
(continued...)

competing concerns in part by Supreme Court decisions on related issues. In *Katz v. United States*, 389 U.S. 347 (1967), the Court held that the protections of the Fourth Amendment extended to circumstances involving electronic surveillance of oral communications without physical intrusion.² The *Katz* Court stated, however, that its holding did not extend to cases involving national security.³ In *United States v. United States District Court*, 407 U.S. 297 (1972) (the *Keith* case), the Court regarded *Katz* as “implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.”⁴ Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President’s power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government’s right to protect itself from unlawful subversion and attack and to the citizen’s right to be secure in his privacy against unreasonable Government intrusion.⁵

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.⁶ Justice Powell emphasized that the case before it “require[d] no judgment on the scope of the President’s surveillance power with respect to the activities of foreign

¹(...continued)

Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

²*Katz v. United States*, 389 U.S. 347, 353 (1967).

³*Id.*, at 359, n. 23.

⁴*United States v. United States District Court*, 407 U.S. 297, 313-14 (1972).

⁵407 U.S. at 299.

⁶*Id.*, at 391-321. Justice Powell also observed that,

National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of “ordinary” crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. “Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power,” *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961). . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect “domestic security.” . . .

powers, within or without the country.”⁷ The Court expressed no opinion as to “the issues which may be involved with respect to activities of foreign powers or their agents.”⁸ However, the guidance which the Court provided in *Keith* with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. The *Keith* Court observed in part:

... We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime.” The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes. Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. . . . It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . . ; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.⁹

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom, Ivanov v.*

⁷*Id.*, at 308.

⁸*Id.*, at 321-22.

⁹407 U.S. at 323-24.

United States, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."

With the passage of the Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified as amended at 50 U.S.C. § 1801 *et seq.*, Congress sought to strike a delicate balance between these interests when the gathering of foreign intelligence involved the use of electronic surveillance.¹⁰ Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12333.¹¹ This report will examine the provisions of FISA which deal with electronic surveillance, in the foreign intelligence context, as well as those applicable to physical searches, the use of pen registers and trap and trace devices under FISA, and access to business records and other tangible things for foreign intelligence purposes. As the provisions of E.O. 12333 to some extent set the broader context within which FISA operates, we will briefly examine its pertinent provisions first.

Executive Order 12333

Under Part 2.3 of E.O. 12333, the agencies within the Intelligence Community are to "collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. . . ." Among the types of information that can be collected, retained or disseminated under this section are:

- (a) Information that is publicly available or collected with the consent of the person concerned;

¹⁰For an examination of the legislative history of P.L. 95-511, see S. Rept. 95-604, Senate Committee on the Judiciary, Parts I and II (Nov. 15, 22, 1977); S. Rept. 95-701, Senate Select Committee on Intelligence (March 14, 1978); H. Rept. 95-1283, House Permanent Select Committee on Intelligence (June 8, 1978); H. Conf. Rept. 95-1720 (Oct. 5, 1978); Senate Reports and House Conference Report are reprinted in 1978 *U.S. Code Cong. & Admin. News* 3904.

¹¹Physical searches for foreign intelligence information are governed by 50 U.S.C. § 1821 *et seq.*, while the use of pen registers and trap and trace devices in connection with foreign intelligence investigations is addressed in 50 U.S.C. § 1841 *et seq.* Access to certain business records for foreign intelligence or international terrorism investigative purposes is covered by 50 U.S.C. § 1861 *et seq.*

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical or communications security investigation;

(i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

In discussing collections techniques, Part 2.4 of E.O. 12333 indicates that agencies within the Intelligence Community are to use

the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. . . .

Part 2.5 of the Executive Order 12333 states that:

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for

law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978 [section 1801 et seq. of this title], shall be conducted in accordance with that Act, as well as this Order.

The Foreign Intelligence Surveillance Act

The Statutory Framework

Electronic surveillance under FISA. The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, as amended, provides a framework for the use of electronic surveillance,¹² physical searches, pen registers and trap and trace devices to acquire foreign intelligence information.¹³ This measure seeks to strike a balance

¹²50 U.S.C. § 1801(f)(2) defines “electronic surveillance” to mean:

- (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any person thereto, if such acquisition occurs in the United States, *but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18*;
- (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
- (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

The italicized portion of Subsection 1801(f)(2) was added by Sec. 1003 of P.L. 107-56.

¹³“Foreign intelligence information” is defined in 50 U.S.C. § 1801(e) to mean:

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
 - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (B) sabotage or international terrorism by a foreign power or an agent of a foreign power;

(continued...)

between national security needs in the context of foreign intelligence gathering and privacy rights.

Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance to acquire foreign intelligence information for up to one year without a court order if two criteria are satisfied. First, to utilize this authority, the Attorney General must certify in writing under oath that:

- (A) the electronic surveillance is solely directed at —
 - (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
 - (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2) or (3) of this title;
- (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
- (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title;¹⁴

¹³(...continued)

- (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
 - (A) the national defense or the security of the United States; or
 - (B) the conduct of the foreign affairs of the United States.

“International terrorism” is defined in 50 U.S.C. § 1801(c) to mean activities that:

- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
- (2) appear to be intended—
 - (A) to intimidate or coerce a civilian population;
 - (B) to influence the policy of a government by intimidation or coercion; or
 - (C) to affect the conduct of a government by assassination or kidnapping;
 and
- (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

“Sabotage” is defined in 50 U.S.C. § 1801(d) to mean “activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States.”

¹⁴Minimization procedures with respect to electronic surveillance are defined in 50 U.S.C. § 1801(h) to mean:

(continued...)

¹⁴(...continued)

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Sec. 314(a)(1) of H. Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002 to accompany H.R. 2883, amended 50 U.S.C. § 1801(h)(4) to change to 72 hours what was previously a 24 hour period beyond which the contents of any communication to which a U.S. person is a party may not be retained absent a court order under 50 U.S.C. § 1805 or a finding by the Attorney General that the information indicates a threat of death or serious bodily injury. The conference version of H.R. 2883 received the approbation of both houses of Congress, and was forwarded to the President on December 18, 2001, for his signature. It became P.L. 107-108.

"United States person" is defined in 50 U.S.C. § 1801(i) to mean

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power" is defined in 50 U.S.C. § 1801(a) to mean:

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(continued...)

....

Second, in order for the President, through the Attorney General, to use this authority

... the Attorney General [must report] such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization and the reason for their becoming effective immediately.

¹⁴(...continued)

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

“Agent of a foreign power” is defined in 50 U.S.C. § 1801(b) to mean:

(1) any person other than a United States person, who--

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who--

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Such electronic surveillance must be conducted only in accordance with the Attorney General's certification and minimization procedures adopted by him. A copy of his certification must be transmitted by the Attorney General to the court established under 50 U.S.C. § 1803(a) (hereinafter the FISC).¹⁵ This certification remains under seal unless an application for a court order for surveillance authority is made under 50 U.S.C. §§ 1801(h)(4) and 1804,¹⁶ or the certification is necessary to determine the legality of the surveillance under 50 U.S.C. § 1806(f).¹⁷ 50 U.S.C. § 1802(a)(2) and (a)(3).

In connection with electronic surveillance so authorized, the Attorney General may direct a specified communications common carrier to furnish all information, facilities, or technical assistance needed for the electronic surveillance to be accomplished in a way that would protect its secrecy and minimize interference with the services provided by the carrier to its customers. 50 U.S.C. § 1802(a)(4)(A). In addition, the Attorney General may direct the specified communications common carrier to maintain any records, under security procedures approved by the Attorney General and the Director of Central Intelligence, concerning the surveillance or the assistance provided which the carrier wishes to retain. 50 U.S.C. § 1802(a)(4)(B). Compensation at the prevailing rate must be made to the carrier by the Government for providing such aid.

If the President, by written authorization, empowers the Attorney General to approve applications to the FISC, an application for a court order may be made pursuant to 50 U.S.C. § 1802(b). A judge receiving such an application may grant an order under 50 U.S.C. § 1805 approving electronic surveillance of a foreign power or an agent of a foreign power to obtain foreign intelligence information. There is an exception to this, however. Under 50 U.S.C. § 1802(b), a court does not have jurisdiction to grant an order approving electronic surveillance directed solely as

¹⁵Under 50 U.S.C. § 1803(a), as amended by Section 208 of P.L. 107-56, the Chief Justice of the United States must publicly designate eleven U.S. district court judges from seven of the United States judicial circuits, of whom no fewer than three must reside within 20 miles of the District of Columbia. These eleven judges constitute the court which has jurisdiction over applications for and orders approving electronic surveillance anywhere within the United States under FISA. If an application for electronic surveillance under this Act is denied by one judge of this court, it may not then be considered by another judge on the court. If a judge denies such an application, he or she must immediately provide a written statement for the record of the reason(s) for this decision. If the United States so moves, this record must then be transmitted under seal to a court of review established under 50 U.S.C. § 1803(b). The Chief Justice also publicly designates the three U.S. district court or U.S. court of appeals judges who together make up the court of review having jurisdiction to review any denial of an order under FISA. If that court determines that an application was properly denied, again a written record of the reason(s) for the court of review's decision must be provided for the record, and the United States may petition for a writ of certiorari to the United States Supreme Court. All proceedings under this Act must be conducted expeditiously, and the record of all proceedings including applications and orders granted, must be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence. 50 U.S.C. § 1803(c).

¹⁶50 U.S.C. § 1804 is discussed at pages 11-15 of this report, *infra*.

¹⁷50 U.S.C. § 1806 is discussed at pages 20-25 of this report, *infra*.

described in 50 U.S.C. § 1802(a)(1)(A) (that is, at acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, or acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power), unless the surveillance may involve the acquisition of communications of a United States person. 50 U.S.C. § 1802(b).

An application for a court order authorizing electronic surveillance for foreign intelligence purposes may be sought under 50 U.S.C. § 1804. An application for such a court order must be made by a federal officer in writing on oath or affirmation to an FISC judge. The application must be approved by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 *et seq.* have been met. Section 1804(a) sets out what must be included in the application:

- (1) the identity of the Federal officer making the application;
- (2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
- (3) the identity, if known, or a description of the target of the electronic surveillance;
- (4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that —
 - (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
 - (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (5) a statement of the proposed minimization procedures;
- (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
- (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate¹⁸ —
 - (A) that the certifying official deems the information sought to be foreign intelligence information;

¹⁸Under Section 1-103 of Executive Order 12139, the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the FBI, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence were designated to make such certifications in support of applications to engage in electronic surveillance for foreign intelligence purposes. Neither these officials nor anyone acting in those capacities may make such certifications unless they are appointed by the President with the advice and consent of the Senate.

- (B) that a *significant*¹⁹ purpose of the surveillance is to obtain foreign intelligence information;
- (C) that such information cannot reasonably be obtained by normal investigative techniques;
- (D) that designates the type of foreign intelligence information being sought according to the categories described in 1801(e) of this title; and
- (E) including a statement of the basis for the certification that —
 - (i) the information sought is the type of foreign intelligence information designated; and
 - (ii) such information cannot reasonably be obtained by normal investigative techniques;

¹⁹ Section 218 of P.L. 107-56 amended the requisite certifications to be made by the Assistant to the President for National Security Affairs, or other designated official (see footnote 18). Heretofore, the certifying official had to certify, among other things, that the purpose of the electronic surveillance under FISA was to obtain foreign intelligence information. Under the new language, the certifying official must certify that a *significant* purpose of such electronic surveillance is to obtain foreign intelligence information. This change may have the effect of somewhat blurring the line between electronic surveillance for foreign intelligence purposes and that engaged in for criminal law enforcement purposes.

Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, *United States v. Megahey*, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), *aff'd* 729 F.2d 1444 (2d Cir. 1982); *United States v. Ott*, 827 F.2d 473, 475 (9th Cir. 1987); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987). See also, *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991), *rehearing and cert. denied*, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); *United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard—i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense—for issuance of a search warrant was violative of the 4th Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); *United States v. Rahman*, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). Cf., *United States v. Bin Laden*, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); *United States v. Bin Laden*, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection. . . . If foreign intelligence collection is merely a purpose and not the *primary* purpose of a search, the exception does not apply.")

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

The application for a court order need not contain the information required in Subsections 1804(6), (7)(E), (8), and (11) above if the target of the electronic surveillance is a foreign power and each of the facilities or places at which surveillance is directed is owned, leased, or exclusively used by that foreign power. However, in those circumstances, the application must indicate whether physical entry is needed to effect the surveillance, and must also contain such information about the surveillance techniques and communications or other information regarding United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures. 50 U.S.C. § 1804(b).

Where an application for electronic surveillance under 50 U.S.C. § 1804(a) involves a target described in 50 U.S.C. § 1801(b)(2),²⁰ the Attorney General must personally review the application if requested to do so, in writing, by the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of Central Intelligence.²¹ The authority to make such a request may not be delegated unless the official involved is disabled or otherwise unavailable.²² Each such official must make appropriate arrangements, in advance, to ensure that such a delegation of authority is clearly established in case of disability or other unavailability.²³ If the Attorney General determines that an application should not be approved, he must give the official requesting the Attorney General's personal review of the application written notice of the determination. Except in cases where the Attorney General is disabled or otherwise unavailable, the responsibility for such a determination may not be delegated. The Attorney General must make advance plans to ensure that the delegation of such responsibility where the Attorney General is disabled or otherwise unavailable is clearly established.²⁴ Notice of the Attorney General's determination that an application should not be approved must indicate

²⁰For a list of those covered in 50 U.S.C. § 1801(b)(2), see footnote 14, *supra*.

²¹50 U.S.C. § 1804(e)(1)(A).

²²50 U.S.C. § 1804(e)(1)(B).

²³50 U.S.C. § 1804(e)(1)(C).

²⁴50 U.S.C. § 1804(e)(2)(A).

what modifications, if any, should be made in the application needed to make it meet with the Attorney General's approval.²⁵ The official receiving the Attorney General's notice of modifications which would make the application acceptable must modify the application if the official deems such modifications warranted. Except in cases of disability or other unavailability, the responsibility to supervise any such modifications is also a non-delegable responsibility.²⁶

If a judge makes the findings required under 50 U.S.C. § 1805(a), then he or she must enter an ex parte order as requested or as modified approving the electronic surveillance. The necessary findings must include that:

- (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
- (2) the application has been made by a Federal officer and approved by the Attorney General;
- (3) on the basis of the facts submitted by the applicant there is probable cause to believe that —
 - (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
 - (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
- (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

In making a probable cause determination under 50 U.S.C. § 1805(a)(3), the judge may consider past activities of the target as well as facts and circumstances relating to the target's current or future activities.²⁷ An order approving an electronic surveillance under Section 1805(c) must:

- (1) specify—
 - (A) the identity, if known, or a description of the target of the electronic surveillance;
 - (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, *if known*;²⁸

²⁵50 U.S.C. § 1804(e)(2)(B).

²⁶50 U.S.C. § 1804(e)(2)(C).

²⁷50 U.S.C. § 1805(b).

²⁸Section 314(a)(2)(A) of H. Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002, to accompany H.R. 2883, added "if known" to the
(continued...)

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the device involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant a specified communication or other common carrier, landlord, custodian, or other specified person, *or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons*, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.²⁹

The italicized portions of Section 1805(c)(1)(B) and Section 1805(c)(2)(B) reflect changes, added by P.L. 107-108 and P.L. 107-56 respectively, intended to provide authority for “multipoint” or “roving” electronic surveillance where the actions of the target of the surveillance, such as switching phones and locations repeatedly, may thwart that surveillance. The Conference Report on H.R. 2338, the Intelligence Authorization Act for Fiscal Year 2002, H. Rept. 107-328, at page 24, provided the following explanation of these changes:

The multipoint wiretap amendment to FISA in the USA PATRIOT Act (section 206) allows the FISA court to issue generic orders of assistance to any

²⁸(...continued)

end of Section 1805(c)(1)(B) before the semi-colon. The conference version of the bill passed both the House and the Senate, and was signed by the President on December 28, 2001.

²⁹50 U.S.C. § 1805(c). The italics in 50 U.S.C. § 1805(c)(2)(B), above, indicates new language added by Section 206 of P.L. 107-56. Where circumstances suggest that a target’s actions may prevent identification of a specified person, this new language appears to permit the Foreign Intelligence Surveillance Court to require a service provider, other common carrier, landlord, custodian or other persons to provide necessary assistance to the applicant for a FISA order for electronic surveillance. The heading to Section 6 of P.L. 107-56 refers to this as “roving surveillance authority.” H. Rept. 107-328 calls this a “multipoint” wiretap. *Intelligence Authorization Act for Fiscal Year 2002*, 107th Cong., 1st Sess., H. Rept. 107-328, Conference Report, at 24 (Dec. 6, 2001).

communications provider or similar person, instead of to a particular communications provider. This change permits the Government to implement new surveillance immediately if the FISA target changes providers in an effort to thwart surveillance. The amendment was directed at persons who, for example, attempt to defeat surveillance by changing wireless telephone providers or using pay phones.

Currently, FISA requires the court to "specify" the "nature and location of each of the facilities or places at which the electronic surveillance will be directed." 50 U.S.C. § 105(c)(1)(B). Obviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and electronic mail may be accessed from any number of locations.

To avoid any ambiguity and clarify Congress' intent, the conferees agreed to a provision which adds the phrase, "if known," to the end of 50 U.S.C. § 1805(c)(1)(B). The "if known" language, which follows the model of 50 U.S.C. § 1805(c)(1)(A), is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.

If the target of the electronic surveillance is a foreign power and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order does not need to include the information covered by Section 1805(c)(1)(C), (D), and (F), but must generally describe the information sought, the communications or activities subject to surveillance, the type of electronic surveillance used, and whether physical entry is needed. 50 U.S.C. § 1805(d).

Such an order may approve an electronic surveillance for the period of time necessary to achieve its purpose or for ninety days, whichever is less, unless the order is targeted against a foreign power. In that event, the order shall approve an electronic surveillance for the period specified in the order or for one year, whichever is less. An order under FISA for surveillance targeted against an agent of a foreign power who acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor, may be for the period specified in the order or 120 days, whichever is less.³⁰ Generally, upon application for an extension, a court may grant an extension of an order on the same basis as an original order. An extension must include new findings made in the same manner as that required for the original order. However, an extension of an order for a surveillance targeting a foreign power that is not a United States person may be for a period of up to one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period involved. In addition, an extension of an order for surveillance targeted at an agent of a foreign power who acts in the United States as an officer or employee of a foreign power or as a member of a group engaged in international terrorism or activities in preparation therefore may be extended to a period not exceeding one year. 50 U.S.C. § 1805(e)(2)(A) and (B).³¹

³⁰50 U.S.C. § 1805(e)(1)(B), as added by Section 207 of P.L. 107-56.

³¹Section 207 of P.L. 107-56 appears to have included a mistaken citation here, referring to (continued...)

Emergency situations are addressed in 50 U.S.C. § 1805(f).³² Notwithstanding other provisions of this subchapter, if the Attorney General reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained and that the factual basis for issuance of an order under this subchapter to approve such surveillance exists, he may authorize electronic surveillance if specified steps are taken. At the time of the Attorney General's emergency authorization, he or his designee must inform an FISC judge that the decision to employ emergency electronic surveillance has been made. An application for a court order under Section 1804 must be made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes emergency electronic surveillance, he must require compliance with the minimization procedures required for the issuance of a judicial order under this subchapter. Absent a judicial order

³¹(...continued)

50 U.S.C. § 1805(d)(2) instead of 50 U.S.C. § 1805(e)(2) (emphasis added). The amending statutory language discussed above appears to reflect an intended change to subsection 1805(e)(2), as there is no existing statutory language readily susceptible to such an amendment in subsection 1805(d)(2). Section 314(c)(1) of P.L. 107-108, the conference version of H.R. 2883, in H. Rept. 107-328, corrected the apparent error from P.L. 107-56, Section 207, so that the reference is now to 50 U.S.C. § 1805(e)(2). The conference version of H.R. 2883 was signed into law by the President on December 28, 2001.

³²50 U.S.C. § 1805(g) authorizes officers, employees, or agents of the United States to conduct electronic surveillance in the normal course of their official duties to test electronic equipment, determine the existence and capability of equipment used for unauthorized electronic surveillance, or to train intelligence personnel in the use of electronic surveillance equipment. Under 50 U.S.C. § 1805(h), the certifications of the Attorney General pursuant to 50 U.S.C. § 1802(a) and applications made and orders granted for electronic surveillance under FISA must be retained for at least 10 years.

Section 225 of P.L. 107-56 appears to create a second subsection 1805(h), which precludes any cause of action in any court "against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA. This immunity provision is included in 50 U.S.C. § 1805, and was denominated "Immunity for Compliance with FISA Wiretap" in Section 225 of the USA PATRIOT Act, both facts which might lead one to conclude that it applied only to electronic surveillance under FISA. However, in H. Rept. 107-328, the conference report accompanying H.R. 2883, which became P.L. 107-108, the conferees expressed the view that "the text of section 225 refers to court orders and requests for emergency assistance 'under this Act,' which makes clear that it applies to physical searches (and pen-trap requests—for which there already exists an immunity provision, 50 U.S.C. § 1842(f)—and subpoenas) as well as electronic surveillance." *Id.* at 25.

Section 314(a)(2)(C) of P.L. 107-108, the conference report version of H.R. 2883, in H. Rept. 107-328, changed subsection (h), which was added to 50 U.S.C. § 1805 by Section 225 of P.L. 107-56, to subsection (i). In addition, Section 314(a)(2)(D) of the conference report version of H.R. 2883 added "for electronic surveillance or physical search" to the end of the newly designated 50 U.S.C. § 1805(i) before the final period. The measure was signed into law by the President on December 28, 2001.

approving the emergency electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after 72 hours from the time of the Attorney General's authorization, whichever is earliest.³³ If no judicial order approving the surveillance is issued, the information garnered may not be received in evidence or otherwise disclosed in any court proceeding, or proceeding in or before any grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof. No information concerning any United States person acquired through such surveillance may be disclosed by any Federal officer or employee without the consent of that person, unless the Attorney General approves of such disclosure or use where the information indicates a threat of death or serious bodily harm to any person.³⁴

³³Section 314(a)(2)(B) of the conference report version of H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002, H. Rept. 107-328, replaced 24 hours with 72 hours in each place that it appears in 50 U.S.C. § 1805(f). The measure was forwarded to the President for his signature on December 18, 2001, and signed into law on December 28, 2001, as P.L. 107-108.

³⁴Some of the provisions dealing with interception of wire, oral, or electronic communications in the context of criminal law investigations, 18 U.S.C. §§ 2510 *et seq.*, may also be worthy of note. With certain exceptions, these provisions, among other things, prohibit any person from engaging in intentional interception; attempted interception; or procuring others to intercept or endeavor to intercept wire, oral, or electronic communication; or intentional disclosure; attempting to disclose; using or endeavoring to use the contents of a wire, oral or electronic communication, knowing or having reason to know that the information was obtained by such an unlawful interception. 18 U.S.C. § 2511. "Person" is defined in 18 U.S.C. § 2510(6) to include "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." Among the exceptions to Section 2511 are two of particular note:

(2)(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(2)(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

Among other things, Section 2512 prohibits any person from intentionally manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing that its design renders it primarily useful for the purpose of the

(continued...)

³⁴(...continued)

surreptitious interception of wire, oral, or electronic communications and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. It also prohibits any person from intentionally sending such a device through the mail or sending or carrying such a device in interstate or foreign commerce, knowing that such surreptitious interception is its primary purpose. Similarly, intentionally advertising such a device, knowing or having reason to know that the advertisement will be sent through the mail or transported in interstate or foreign commerce is foreclosed. Again an exception to these general prohibitions in Section 2512 may be of particular interest:

(2) It shall not be unlawful under this section for—

(a) . . .

(b) an officer, agent, or employee of, or a person under contract with, the United States . . . in the normal course of the activities of the United States . . . ,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

In addition, Section 107 of the Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1858, October 21, 1986, [which enacted 18 U.S.C. §§ 1367, 2621, 2701 to 2711, 3117, and 3121 to 3126; and amended 18 U.S.C. §§ 2232, 2511-2513, and 2516-2520], provided generally that, “[n]othing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.” It also stated:

(b) Certain Activities Under Procedures Approved by the Attorney General.—Nothing in chapter 119 [interception of wire, oral or electronic communications] or chapter 121 [stored wire and electronic communications and transactional records access] of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.]; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.].

In addition, Chapter 121 of title 18 of the United States Code deals with stored wire and electronic communications and transactional records. Under 18 U.S.C. § 2701, intentionally accessing without authorization a facility through which an electronic communication service is provided, or intentionally exceeding an authorization to access such a facility and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such system is prohibited. Upon compliance with statutory requirements in 18 U.S.C. § 2709, the Director of the FBI

(continued...)

The uses to which information gathered under FISA may be put are addressed under 50 U.S.C. § 1806.³⁵ Under these provisions, disclosure, without the

³⁴(...continued)

or his designee in a position not lower than deputy Assistant Director may seek access to telephone toll and transactional records for foreign counterintelligence purposes. The FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the FBI, and, "with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency." 18 U.S.C. § 2709(d).

³⁵The provisions of Section 1806 are as follows:

(a) Compliance with minimization procedures; privileged communications; lawful purposes

Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with or in violation of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced

(continued...)

³⁵(...continued)

or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio

(continued...)

consent of the person involved, of information lawfully acquired under FISA which concerns a United States person must be in compliance with the statutorily mandated minimization procedures. Communications which were privileged when intercepted remain privileged. Where information acquired under FISA is disclosed for law enforcement purposes, neither that information nor any information derived therefrom may be used in a criminal proceeding without prior authorization of the Attorney General. If the United States Government intends to disclose information acquired under FISA or derived therefrom in any proceeding before a court, department, officer

³⁵(...continued)

communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application or on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

- (1) the fact of the application;
- (2) the period of the surveillance; and
- (3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forgo ordering the serving of the notice required under this subsection.

(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against--

- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
- (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) [50 U.S.C. § 1804(a)(7)(B) (referring to a certification by the Assistant to the President for National Security Affairs or other designated certifying authority "that a significant purpose of the surveillance is to obtain foreign intelligence information")] or the entry of an order under section 105 [50 U.S.C. § 1805].

Subsection 1806(k) was added by Section 504 of P.L. 107-56. The term "aggrieved person," as used in connection with electronic surveillance under FISA, is defined under 50 U.S.C. § 1801(k) to mean "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."

regulatory body or other authority of the United States against an aggrieved person,³⁶ then the Government must give prior notice of its intent to disclose to the aggrieved person and to the court or other authority involved. Similarly, a State or political subdivision of a State that intends to disclose such information against an aggrieved person in a proceeding before a State or local authority must give prior notice of its intent to the aggrieved person, the court or other authority, and the Attorney General.

Section 1806 also sets out in camera and ex parte district court review procedures to be followed where such notification is received, or where the aggrieved person seeks to discover or obtain orders or applications relating to FISA electronic surveillance, or to discover, obtain, or suppress evidence or information obtained or derived from the electronic surveillance, and the Attorney General files an affidavit under oath that such disclosure would harm U.S. national security. The focus of this review would be to determine whether the surveillance was lawfully conducted and authorized. Only where needed to make an accurate determination of these issues does the section permit the court to disclose to the aggrieved person, under appropriate security measures and protective orders, parts of the application, order, or other materials related to the surveillance. If, as a result of its review, the district court determines that the surveillance was unlawful, the resulting evidence must be suppressed.³⁷ If the surveillance was lawfully authorized and conducted, the motion

³⁶For the definition of “aggrieved person” as that term is used with respect to targets of electronic surveillance under FISA, see fn. 35, *supra*.

³⁷*But see, United States v. Thomson*, 752 F. Supp. 75, 77 (W.D. N.Y. 1990), stating that,

If the Court determines that the surveillance was unlawfully authorized or conducted, it must order disclosure of the FISA material. 50 U.S.C. § 1806(g) In *United States v. Belfield*, 692 F.2d 141 (D.C. Cir. 1982), the court stated that: “even when the government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the FISA surveillance material to ensure that no fruits thereof are being used against him.” *Id.* at 146.

It may be noted that the Section 1806(g) does not state that a court must order disclosure of the FISA material if the court finds that the FISA electronic surveillance was unlawfully authorized or conducted. Rather, the provision in question states in pertinent part that, “If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. . . .” While a district court will normally consider in camera and ex parte a motion to suppress under Subsection 1806(e) or other statute or rule to discover, disclose, or suppress information relating to a FISA electronic surveillance, Subsection 1806(f) does permit a district court, in determining the legality of a FISA electronic surveillance, to disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance only to the extent necessary to make an accurate determination of the legality of the surveillance. *Belfield* indicated that a criminal defendant may seek to discover FISA surveillance material to ensure that no fruits of an illegal surveillance are

(continued...)

of the aggrieved person must be denied except to the extent that due process requires discovery or disclosure. Resultant court orders granting motions or requests of the aggrieved person for a determination that the surveillance was not lawfully conducted or authorized and court orders requiring review or granting disclosure are final orders binding on all Federal and State courts except a U.S. Court of Appeals and the U.S. Supreme Court.

If the contents of any radio communication are unintentionally acquired by an electronic, mechanical, or other surveillance device in circumstances where there is a reasonable expectation of privacy and where a warrant would be required if the surveillance were to be pursued for law enforcement purposes, then the contents must be destroyed when recognized, unless the Attorney General finds that the contents indicate a threat of death or serious bodily harm to any person.

As noted above, Section 1805 provides for emergency electronic surveillance in limited circumstances, and requires the subsequent prompt filing of an application for court authorization to the FISC in such a situation. Under Section 1806, if the application is unsuccessful in obtaining court approval for the surveillance, notice must be served upon any United States person named in the application and such other U.S. persons subject to electronic surveillance as the judge determines, in the exercise of his discretion, is in the interests of justice. This notice includes the fact of the application, the period of surveillance, and the fact that information was or was not obtained during this period. Section 1806 permits postponement or suspension of service of notice for up to ninety days upon ex parte good cause shown. Upon a further ex parte showing of good cause thereafter, the court will forego ordering such service of notice.³⁸

³⁷(...continued)

being used against him, but it appears to stop short of saying that in every instance where the court finds an illegal surveillance disclosure must be forthcoming. "The language of section 1806(f) clearly anticipates that an ex parte, in camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary." *Belfield*, *supra*, 692 F.2d at 147. See also, *United States v. Squillacote*, 221 F.3d 542, 552-554 (4th Cir. 2000), *cert. denied*, ___ U.S. ___, 2001 U.S. LEXIS 2915 (April 16, 2001).

³⁸ Cf., *United States Attorney's Manual*, §§ 1-2.106 (Office of Intelligence Policy and Review organization and functions). This section indicates, in part, that the Office of Intelligence Policy and Review

... prepares certifications and applications for electronic surveillance under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., and represents the United States before the United States Foreign Intelligence Surveillance Court. It processes requests for Attorney General Authority to use FISA material in adjudicatory proceedings and assists in responding to challenges to the legality of FISA surveillances.

See also, 28 C.F.R. § 0.33 (functions of the Counsel for Intelligence Policy); *United States Attorneys' Criminal Resource Manual*, §§ 1073 (FISA-50 U.S.C. § 1809) and 1075 (elements of the offense under 50 U.S.C. § 1809(a)); cf., *United States Attorney's Manual* § 9-7.301 (consensual monitoring in the context of electronic surveillance).

P.L. 107-56, Section 504, added a new subsection 1806(k)(1). Under this new subsection, federal officers who conduct electronic surveillance to acquire foreign intelligence under FISA are permitted to consult with Federal law enforcement officers to coordinate investigative efforts or to protect against—

- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
- (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

This new subsection indicates further that such coordination would not preclude certification as required by 50 U.S.C. § 1804(a)(7)(B) or entry of a court order under 50 U.S.C. § 1805.

Reporting requirements are included in Sections 1807 and 1808. Under Section 1807, each year in April, the Attorney General is directed to transmit to the Administrative Office of the United States Courts and to the Congress a report covering the total number of applications made for orders and extensions of orders approving electronic surveillance under FISA during the previous year, and the total number of orders and extensions granted, modified, or denied during that time period. Section 1808(a) requires the Attorney General to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence semiannually about all electronic surveillance under FISA.³⁹ Each such report must contain a description of each criminal case in which information acquired under FISA “has been passed for law enforcement purposes” during the period covered by the report, and each criminal case in which information acquired under FISA has been authorized to be used at trial during the reporting period.⁴⁰

Section 1809 provides criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute; or for disclosing or using information obtained under color of law by electronic surveillance, knowing or having reason to know that surveillance was not authorized by statute.⁴¹ The

³⁹Subsection 1808(b) directed these committees to report annually for five years after the date of enactment to the House and the Senate respectively concerning implementation of FISA, including any recommendations for amendment, repeal, or continuation without amendment. P.L. 106-567, Title VI, Sec. 604(b) (Dec. 27, 2000), 114 Stat. 2853, required the Attorney General to submit to the Senate Select Committee on Intelligence, the Senate Judiciary Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee a report on the authorities and procedures utilized by the Department of Justice to determine whether or not to disclose information acquired under FISA for law enforcement purposes. 50 U.S.C. § 1806 note.

⁴⁰50 U.S.C. § 1808(a)(2).

⁴¹Section 1075 of the *United States Attorneys' Criminal Resource Manual* indicates that Section 1809(a) “reaches two distinct acts: (1) engaging in unauthorized electronic surveillance under color of law; and (2) using or disclosing information obtained under color of law through unauthorized electronic surveillance. Each offense involves an “intentional” (continued...) ”

provision makes it a defense to prosecution under this subsection if the defendant is a law enforcement officer or investigative officer in the course of his official duties and the electronic surveillance was authorized by and conducted under a search warrant or court order of a court of competent jurisdiction. Section 1809 provides for Federal jurisdiction over such an offense if the defendant is a Federal officer or employee at the time of the offense. Civil liability is also provided for under Section 1810, where an aggrieved person, who is neither a foreign power nor an agent of a foreign power, has been subjected to electronic surveillance, or where information gathered by electronic surveillance about an aggrieved person has been disclosed or used in violation of Section 1809.

Finally, Section 1811 provides that, notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order to acquire foreign intelligence information for up to 15 calendar days following a declaration of war by Congress.

Physical searches for foreign intelligence gathering purposes.

Physical searches for foreign intelligence purposes are addressed in 50 U.S.C. § 1821 *et seq.*⁴² While tailored for physical searches, the provisions in many respects follow a pattern similar to that created for electronic surveillance. The definitions from 50 U.S.C. § 1801 for the terms “foreign power,” “agent of a foreign power,” “international terrorism,” “sabotage,” “foreign intelligence information,” “Attorney General,” “United States person,” “United States,” “person,” and “State” also apply to foreign intelligence physical searches except where specifically provided otherwise. A “physical search” under this title means:

any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) “electronic surveillance”, as defined in section 1801(f) of this title [50 U.S.C.], or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in

⁴¹(...continued)

state of mind and unauthorized “electronic surveillance.” Section 1075 further notes:

Even though none of these elements mentions foreign intelligence, one court has explained that “the FISA applies only to surveillance designed to gather information relevant to foreign intelligence.” *United States v. Koyomejian*, 970 F. 2d 536, 540 (9th Cir. 1992) (en banc), cert denied, 506 U.S. 1005 (1992). In fact, all applications for an order from the Foreign Intelligence Surveillance Court require a certification from a presidentially designated official that the purpose of the surveillance is to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7).

⁴²The physical search provisions of FISA were added as Title III of that Act by P.L. 103-359, Title VIII, on October 14, 1994, 108 Stat. 3443. Some of these provisions were subsequently amended by P.L. 106-567, Title VI, on December 27, 2000, 114 Stat. 2852-53; and by P.L. 107-56.

accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 1801(f) of this title.⁴³

Minimization procedures also apply to physical searches for foreign intelligence purposes. Those defined under 50 U.S.C. § 1821(4) are tailored to such physical searches, and like those applicable to electronic surveillance under 50 U.S.C. § 1801(h), these procedures are designed to minimize acquisition and retention, and to prohibit dissemination of nonpublicly available information concerning unconsenting U.S. persons, consistent with the needs of the United States to obtain, produce and disseminate foreign intelligence.⁴⁴

Under 50 U.S.C. § 1822, the President, acting through the Attorney General may authorize physical searches to acquire foreign intelligence information without a court order for up to one year if the Attorney General certifies under oath that the search is solely directed at premises, property, information or materials owned by or under the open and exclusive control of a foreign power or powers.⁴⁵ For these purposes,

⁴³50 U.S.C. § 1821(5).

⁴⁴Specifically, 50 U.S.C. § 1821(4) defines “minimization procedures” with respect to physical search to mean:

- (A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
- (B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand such foreign intelligence information or assess its importance;
- (C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
- (D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours; unless a court order under section 1824 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Section 314(a)(3) of P.L. 107-108, the conference version of the Intelligence Authorization Act of 2002, H.R. 2883, from H. Rept. 107-328, changed the previous 24 hour period in the minimization procedures under 50 U.S.C. § 1821(4)(D) to a 72 hour period. The bill passed both houses of Congress and was signed by the President on December 28, 2001.

⁴⁵The president provided such authority to the Attorney General by Executive Order 12949, (continued...)

“foreign power or powers” means a foreign government or component of a foreign government, whether or not recognized by the United States, a faction of a foreign nation or nations, not substantially composed of U.S. persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.⁴⁶ In addition, the Attorney General must certify that there is no substantial likelihood that the physical search will involve the premises, information, material or property of a U.S. person, and that the proposed minimization procedures with respect to the physical search are consistent with 50 U.S.C. § 1821(4)(1)-(4).⁴⁷ Under normal circumstances, these minimization procedures and any changes to them are reported to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence by the Attorney General at least 30 days before their effective date. However, if the Attorney General determines that immediate action is required, the statute mandates that he advise these committees immediately of the minimization procedures and the need for them to become effective immediately. In addition, the Attorney General must assess compliance with these minimization procedures and report such assessments to these congressional committees.

The certification of the Attorney General for a search under 50 U.S.C. § 1822 is immediately transmitted under seal to the Foreign Intelligence Surveillance Court, and maintained there under security measures established by the Chief Justice of the United States with the Attorney General’s concurrence, in consultation with the Director of Central Intelligence. Such a certification remains under seal unless one of two circumstances arise: (1) either an application for a court order with respect to the physical search is made to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1821(4) (dealing with minimization procedures) and § 1823 (dealing with the process by which a federal officer, with the approval of the Attorney General, may apply for an order from the FISC approving a physical search for foreign intelligence gathering purposes); or (2) the certification is needed to determine the legality of a physical search under 50 U.S.C. § 1825 (dealing with use of the information so gathered).

In connection with physical searches under 50 U.S.C. § 1822, the Attorney General may direct a landlord, custodian or other specified person to furnish all necessary assistance needed to accomplish the physical search in a way that would both protect its secrecy and minimize interference with the services such person provides the target of the search. Such person may also be directed to maintain any records regarding the search or the aid provided under security procedures approved by the Attorney General and the Director of Central Intelligence. The provision of

⁴⁵(...continued)

Section 1, 60 *Fed. Reg.* 8169 (February 9, 1995), if the Attorney General makes the certifications necessary under 50 U.S.C. § 1822(a)(1).

⁴⁶See 50 U.S.C. § 1801(a)(1), (2), or (3).

⁴⁷While this is the citation cross-referenced in Section 1822, it appears that the cross-reference should read 50 U.S.C. § 1821(4)(A)-(D).

any such aid must be compensated by the Government.⁴⁸ As in the case of applications for electronic surveillance under FISA, the Foreign Intelligence Surveillance Court (FISC) has jurisdiction to hear applications and grant applications with respect to physical searches under 50 U.S.C. § 1821 *et seq.* No FISC judge may hear an application already denied by another FISC judge. If an application for an order authorizing a physical search under FISA is denied, the judge denying the application must immediately provide a written statement of reasons for the denial. If the United States so moves, the record is then transmitted under seal to the court of review established under 50 U.S.C. § 1803(b). If the court of review determines that the application was properly denied, it, in turn, must provide a written statement of the reasons for its decision, which must be transmitted under seal to the Supreme Court upon petition for certiorari by the United States.⁴⁹ Any of the proceedings with respect to an application for a physical search under FISA must be conducted expeditiously, and the record of such proceedings must be kept under appropriate security measures.

The requirements for application for an order for a physical search under FISA are included in 50 U.S.C. § 1823. While tailored to a physical search, the requirements strongly parallel those applicable to electronic surveillance under 50 U.S.C. § 1804(a)(1)-(9).⁵⁰ Like Section 1804(a)(7)(B) with respect to required

⁴⁸50 U.S.C. § 1822(a)(4).

⁴⁹50 U.S.C. § 1822(c), (d).

⁵⁰Each application for an order approving such a physical search, having been approved by the Attorney General based upon his understanding that the application satisfies the criteria and requirements of 50 U.S.C. § 1821 *et seq.*, must be made by a Federal officer in writing upon oath or affirmation to a FISC judge. Under subsection (a) of Section 1823, the application must include:

- (1) the identity of the Federal officer making the application;
 - (2) the authority conferred on the Attorney General by the President and the approval of the Attorney General to make the application;
 - (3) the identity, if known, or a description of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
 - (4) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that—
 - (A) the target of the physical search is a foreign power or an agent of a foreign power;
 - (B) the premises or property to be searched contains foreign intelligence information; and
 - (C) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;
 - (5) a statement of the proposed minimization procedures;
 - (6) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;
 - (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the
- (continued...)

certifications for an application for electronic surveillance under FISA, Section 1823(a)(7)(B) was amended by P.L. 107-56, Section 218, to require that the Assistant to the President for National Security Affairs or designated executive branch official⁵¹ certify, among other things, that a significant purpose (rather than “that the purpose”) of the physical search is to obtain foreign intelligence information.⁵² Section 1823(d) also parallels Section 1804(c) (dealing with requirements for some applications for electronic surveillance under FISA), in that, if requested in writing by the Director of

⁵⁰(...continued)

advice and consent of the Senate—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the search is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);

(8) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information; and

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, premises, or property specified in the application, and the action taken on each previous application.

Under Section 1823(b), the Attorney General may require any other affidavit or certification from any other officer in connection with an application for a physical search that he deems appropriate. Under Section 1823(c), the FISC judge to whom the application is submitted may also require that the applicant provide other information as needed to make the determinations necessary under 50 U.S.C. § 1824.

⁵¹In Section 2 of E.O. 12949, 60 *Fed. Reg.* 8169 (February 9, 1995), the President authorized the Attorney General to approve applications to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1823, to obtain court orders for physical searches for the purpose of collecting foreign intelligence information. In Section 3 of that executive order, the President designated the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence to make the certifications required by 50 U.S.C. § 1823(a)(7), in support of an application for a court order for a physical search for foreign intelligence purposes. None of these officials may exercise this authority to make the appropriate certifications unless he or she is appointed by the President, with the advice and consent of the Senate.

⁵²As in the case of the change from “the purpose” to “a significant purpose” in the case of electronic surveillance, the parallel language change in Section 1823 with respect to physical searches may also have the effect of blurring the distinction between physical searches for foreign intelligence purposes and those engaged in for law enforcement purposes.

the FBI, the Secretary of Defense, the Secretary of State, or the DCI,⁵³ the Attorney General must personally review an application for a FISA physical search if the target is one described by Section 1801(b)(2). 50 U.S.C. § 1801(b)(2) deals with targets who knowingly engage in clandestine intelligence gathering activities involving or possibly involving violations of federal criminal laws by or on behalf of a foreign power; targets who, at the direction of an intelligence service or network of a foreign power, engage in other clandestine intelligence activities involving or potentially involving federal crimes by or on behalf of a foreign power; targets who knowingly engage in sabotage or international terrorism, activities in preparation for sabotage or international terrorism, or activities on behalf of a foreign power; targets who knowingly aid, abet, or conspire with anyone to engage in any of the previously listed categories of activities; or targets who knowingly enter the United States under false identification by or on behalf of a foreign power or who assume a false identity on behalf of a foreign power while present in the United States.⁵⁴

Should the Attorney General, after reviewing an application, decide not to approve it, he must provide written notice of his determination to the official requesting the review of the application, setting forth any modifications needed for the Attorney General to approve it. The official so notified must supervise the making of the suggested modifications if the official deems them warranted. Unless the Attorney General or the official involved is disabled or otherwise unable to carry out his or her respective responsibilities under Section 1823, those responsibilities are non-delegable.

As in the case of the issuance of an order approving electronic surveillance under 50 U.S.C. § 1805(a), certain findings by the FISC judge are required before an order may be forthcoming authorizing a physical search for foreign intelligence information under 50 U.S.C. § 1824(a). Once an application under Section 1823 has been filed, an FISC judge must enter an ex parte order, either as requested or as modified, approving the physical search if the requisite findings are made. These include findings that:

- (1) the President has authorized the Attorney General to approve applications for physical searches for foreign intelligence purposes;
- (2) the application has been made by a Federal officer and approved by the Attorney General;
- (3) on the basis of the facts submitted by the applicant there is probable cause to believe that—
 - (A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
 - (B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;

⁵³The authority of these officials to make such a written request is non-delegable except where such official is disabled or unavailable. Each must make provision in advance for delegation of this authority should he or she become disabled or unavailable. 50 U.S.C. § 1823(d)(1)(B) and (C).

⁵⁴See fn. 12, *supra*.

- (4) the proposed minimization procedures meet the definition of minimization contained in this subchapter; and
- (5) the application which has been filed contains all statements and certifications required by section 1823 of this title, and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1823(a)(7)(E) of this title and any other information furnished under section 1823(c) of this title.

Like Section 1805(b) regarding electronic surveillance under FISA, a FISC judge making a probable cause determination under Section 1824 may consider the target's past activities, plus facts and circumstances pertinent to the target's present or future activities.⁵⁵

As in the case of an order under 50 U.S.C. § 1805(c) with respect to electronic surveillance, an order granting an application for a physical search under FISA must meet statutory requirements in 50 U.S.C. § 1824(c) as to specifications and directions. An order approving a physical search must specify:

- (A) the identity, if known, or a description of the target of the physical search;
- (B) the nature and location of each of the premises of property to be searched;
- (C) the type of information, material, or property to be seized, altered, or reproduced;
- (D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and
- (E) the period of time during which the physical searches are approved;

In addition, the order must direct:

- (A) that the minimization procedures be followed;
- (B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing to the target of the physical search;
- (C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the search or the aid furnished that such person wishes to retain;
- (D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and
- (E) that the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.⁵⁶

⁵⁵50 U.S.C. § 1824(b).

⁵⁶50 U.S.C. § 1824(c)(1), (2).

Subsection 1824(d) sets the limits on the duration of orders under this section and makes provision for extensions of such orders if certain criteria are met.⁵⁷ Subsection 1824(e) deals with emergency orders for physical searches. It permits the Attorney General, under certain circumstances, to authorize execution of a physical search if the Attorney General or his designee informs a FISC judge that the decision to execute an emergency search has been made, and an application under 50 U.S.C. § 1821 *et seq.* is made to that judge as soon as possible, within 72 hours⁵⁸ after the Attorney General authorizes the search. The Attorney General's decision to authorize such a search must be premised upon a determination that "an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence information before an order authorizing such search can with due diligence be obtained," and "the factual basis for issuance of an order under this title [50 U.S.C.

⁵⁷P.L. 107-56, Section 207(a)(2), amended 50 U.S.C. § 1824(d)(1) so that it provided:

(1) An order under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that (A) an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a) [50 U.S.C. § 1801(b)(1)(A)], for the period specified in the application or for one year, whichever is less, and (B) *an order under this section for a physical search against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)] may be for the period specified in the application or for 120 days, whichever is less.*

The language in italics reflects the changes made by P.L. 107-56. The 90 day time period reflected in the first sentence replaced earlier language which provided for forty-five days.

Section 207(b)(2) of P.L. 107-56 amended 50 U.S.C. § 1824(d)(2) to provide:

(2) Extensions of an order issued under this title [50 U.S.C. §§ 1821 *et seq.*] may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in section 101(a)(5) or (6) [50 U.S.C. § 1801(a)(5) or (6)], or against a foreign power, as defined in section 101(a)(4) [50 U.S.C. § 1801(a)(4)], that is not a United States person, *or against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)]*, may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(Emphasis added.) Under subsection 1824(d)(3), the judge, at or before the end of the time approved for a physical search or for an extension, or at any time after the physical search is carried out, may review circumstances under which information regarding U.S. persons was acquired, retained, or disseminated to assess compliance with minimization techniques.

⁵⁸Section 314(a)(4) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, amended 50 U.S.C. § 1824(e) by striking "24 hours" where it occurred and replacing it with "72 hours."

§ 1821 *et seq.*] to approve such a search exists.”⁵⁹ If such an emergency search is authorized by the Attorney General, he must require that the minimization procedures required for issuance of a judicial order for a physical search under 18 U.S.C. § 1821 *et seq.* be followed.⁶⁰ If there is no judicial order for a such a physical search, then the search must terminate on the earliest of the date on which the information sought is obtained, the date on which the application for the order is denied, or the expiration of the 72 hour period from the Attorney General’s authorization of the emergency search.⁶¹ If an application for approval is denied or if the search is terminated and no order approving the search is issued, then neither information obtained from the search nor evidence derived from the search may be used in evidence or disclosed in any

. . . trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 302 [50 U.S.C. § 1822].⁶²

Subsection 1824(f) requires retention of applications made and orders granted under 50 U.S.C. § 1821 *et seq.*, for a minimum of 10 years from the date of the application.

Like 50 U.S.C. § 1806 with respect to electronic surveillance under FISA, 50 U.S.C. § 1825 restricts and regulates the uses of information secured under a FISA physical search. Such information may only be used or disclosed by Federal officers or employees for lawful purposes. Federal officers and employees must comply with minimization procedures if they use or disclose information gathered from a physical search under FISA concerning a United States person.⁶³ If a physical search involving the residence of a United States person is authorized and conducted under 50 U.S.C. § 1824, and at any time thereafter the Attorney General determines that there is no national security interest in continuing to maintain the search’s secrecy, the Attorney General must provide notice to the United States person whose residence was searched. This notice must include both the fact that the search pursuant to FISA was conducted and the identification of any property of that person which was seized, altered, or reproduced during the search.⁶⁴ Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1821 *et seq.*, must be accompanied by a

⁵⁹50 U.S.C. § 1824(e)(1)(A)(i) and (ii). See fn.58, *supra*, regarding substitution of “72 hours” for “24 hours” in Subsection 50 U.S.C. § 1824(e)(3)(C) by P.L. 107-108, Sec. 314(a)(4).

⁶⁰50 U.S.C. § 1824(e)(2).

⁶¹50 U.S.C. § 1824(e)(3).

⁶²50 U.S.C. § 1824(e)(4).

⁶³50 U.S.C. § 1825(a).

⁶⁴50 U.S.C. § 1825(b).

statement that such information and any derivative information may only be used in a criminal proceeding with advance authorization from the Attorney General.⁶⁵

The notice requirements relevant to intended use or disclosure of information gleaned from a FISA physical search or derivative information, are similar to those applicable where disclosure or use of information garnered from electronic surveillance is intended. If the United States intends to use or disclose information gathered during or derived from a FISA physical search in a trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body or other authority of the United States against an aggrieved person, the United States must first give notice to the aggrieved person, and the court or other authority.⁶⁶ Similarly, if a State or political subdivision of a state intends to use or disclose any information obtained or derived from a FISA physical search in any trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body, or other State or political subdivision against an aggrieved person, the State or locality must notify the aggrieved person, the pertinent court or other authority where the information is to be used, and the Attorney General of the United States of its intention to use or disclose the information.⁶⁷ An aggrieved person may move to suppress evidence obtained or derived from a FISA physical search on one of two grounds: that the information was unlawfully acquired; or that the physical search was not made in conformity with an order of authorization or approval. Such a motion to suppress must be made before the trial, hearing or other proceeding involved unless the aggrieved person had no opportunity to make the motion or was not aware of the grounds of the motion.⁶⁸

In camera, ex parte review by a United States district court may be triggered by receipt of notice under Subsections 1825(d) or (e) by a court or other authority; the making of a motion to suppress by an aggrieved person under Subsection 1825(f); or the making of a motion or request by an aggrieved person under any other federal or state law or rule before any federal or state court or authority to discover or obtain applications, orders, or other materials pertaining to a physical search authorized under FISA or to discover, obtain, or suppress evidence or information obtained or derived from a FISA physical search. If the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm U.S. national security, the U.S. district court receiving notice or before whom a motion or request is pending, or, if the motion is made to another authority, the U.S. district court in the same district as that authority, shall review in camera and ex parte the application, order, and such other materials relating to the physical search at issue needed to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. If the court finds it necessary to make an accurate determination of the

⁶⁵50 U.S.C. § 1825(c).

⁶⁶50 U.S.C. § 1825(d). “Aggrieved person,” as defined in 50 U.S.C. § 1821(2), “means a person whose premises, property, information, or material is the target of a physical search or any other person whose premises, property, information, or material was subject to physical search.”

⁶⁷50 U.S.C. § 1825(e).

⁶⁸50 U.S.C. § 1825(f).

legality of the search, the court may disclose portions of the application, order, or other pertinent materials to the aggrieved person under appropriate security procedures and protective orders, or may require the Attorney General to provide a summary of such materials to the aggrieved person.⁶⁹

If the U.S. district court makes a determination that the physical search was not lawfully authorized or conducted, then it must “suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person.” If, on the other hand, the court finds that the physical search was lawfully authorized or conducted, the motion of the aggrieved person will be denied except to the extent that due process requires discovery or disclosure.⁷⁰

If the U.S. district court grants a motion to suppress under 50 U.S.C. § 1825(h); deems a FISA physical search unlawfully authorized or conducted; or orders review or grants disclosure of applications, orders or other materials pertinent to a FISA physical search, that court order is final and binding on all federal and state courts except a U.S. Court of Appeals or the U.S. Supreme Court.⁷¹

As a general matter, where an emergency physical search is authorized under 50 U.S.C. § 1824(d), and a subsequent order approving the resulting search is not obtained, any U.S. person named in the application and any other U.S. persons subject to the search that the FISC judge deems appropriate in the interests of justice must be served with notice of the fact of the application and the period of the search, and must be advised as to whether information was or was not obtained during that period.⁷² However, such notice may be postponed or suspended for a period not to exceed 90 days upon an ex parte showing of good cause to the judge, and, upon further good cause shown, the court must forego such notice altogether.⁷³

Section 504(b) of P.L. 107-56, added a new 50 U.S.C. § 1825(k) to the statute, which deals with consultation by federal officers doing FISA searches with federal law enforcement officers. Under this new language, federal officers “who conduct physical searches to acquire foreign intelligence information” under 50 U.S.C. § 1821 *et seq.*, may consult with federal law enforcement officers:

- ... to coordinate efforts to investigate or protect against
 - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

⁶⁹50 U.S.C. § 1825(g).

⁷⁰50 U.S.C. § 1825(h).

⁷¹50 U.S.C. § 1825(i).

⁷²50 U.S.C. § 1825(j)(1).

⁷³50 U.S.C. § 1825(j)(2).

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.⁷⁴

Such coordination does not preclude certification required under 50 U.S.C. § 1823(a)(7) or entry of an order under 50 U.S.C. § 1824.⁷⁵

50 U.S.C. § 1826 provides for semiannual congressional oversight of physical searches under FISA. The Attorney General is directed to "fully inform" the permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate with respect to all physical searches conducted under 50 U.S.C. § 1821 *et seq.* Also on a semiannual basis, the Attorney General is required to provide a report to those committees and to the House and Senate Judiciary Committees setting forth: the total number of applications for orders approving FISA physical searches during the preceding 6 month period; the total number of those orders granted, modified, or denied; the number of such physical searches involving the residences, offices, or personal property of United States persons; and the number of occasions, if any, the Attorney General gave notice under 50 U.S.C. § 1825(b).⁷⁶

Section 1827 imposes criminal sanctions for intentionally executing a physical search for foreign intelligence gathering purposes under color of law within the United States except as authorized by statute. In addition, criminal penalties attach to a conviction for intentionally disclosing or using information obtained by a physical search under color of law within the United States for the purpose of gathering intelligence information, where the offender knows or has reason to know that the information was obtained by a physical search not authorized by statute. In either case, this section provides that a person convicted of such an offense faces a fine of not more than \$10,000,⁷⁷ imprisonment for not more than 5 years or both. Federal jurisdiction attaches where the offense is committed by an officer or employee of the United States. It is a defense to such a prosecution if the defendant was a law enforcement or investigative officer engaged in official duties and the physical search was authorized and conducted pursuant to a search warrant or court order by a court of competent jurisdiction.

In addition, an aggrieved person other than a foreign power or an agent of a foreign power as defined under section 1801(a) or 1801(b)(1)(A),⁷⁸ whose premises, property, information, or material within the United States was physically searched under FISA; or about whom information obtained by such a search was disclosed or used in violation of 50 U.S.C. § 1827, may bring a civil action for actual damages,

⁷⁴50 U.S.C. § 1825(k)(1).

⁷⁵50 U.S.C. § 1825(k)(2).

⁷⁶See fn. 64, *supra*, and accompanying text.

⁷⁷This section was added in 1994 as Title III, Section 307 of P.L. 95-511, by P.L. 103-359, Title VIII, § 807(a)(3), 108 Stat. 3452. If a fine were to be imposed under the general fine provisions 18 U.S.C. § 3571, rather than under the offense provision, the maximum fine would be \$250,000 for an individual.

⁷⁸For definitions, see fn. 14, *supra*.

punitive damages, and reasonable attorney's fees and other investigative and litigation costs reasonably incurred.⁷⁹

In times of war, the President, through the Attorney General, may authorize physical searches under FISA without a court order to obtain foreign intelligence information for up to 15 days following a declaration of war by Congress.⁸⁰

Pen registers or trap and trace devices⁸¹ used for foreign intelligence gathering purposes. Title IV of FISA, 50 U.S.C. § 1841 *et seq.*, was added in 1998, significantly amended by P.L. 107-56,⁸² and amended further by Section 314(5) of P.L. 107-108. Under 50 U.S.C. § 1842(a)(1), notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may apply for an order or extension of an order authorizing or approving the installation and use of a pen register or trap and trace device "*for any investigation to protect against international terrorism or clandestine intelligence activities, provided such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution*" conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to E.O. 12333 or a successor order.⁸³ This authority is separate from the authority to conduct electronic surveillance under 50 U.S.C. § 1801 *et seq.*⁸⁴

⁷⁹50 U.S.C. § 1828. Actual damages are defined to be "not less than liquidated damages of \$1,000 or \$100 per day for each violation, whichever is greater." 50 U.S.C. § 1828(1).

⁸⁰50 U.S.C. § 1829.

⁸¹Under 50 U.S.C. § 1841(2), the terms "pen register" and "trap and trace device" are given the meanings in 18 U.S.C. § 3127. Under Section 3127, "pen register"

... means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

As defined by 18 U.S.C. § 3127(4), "trap and trace device" "means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 50 U.S.C. § 1841 is the section that defines terms applicable to the pen register and trap and trace device portions of FISA.

⁸²Title IV of FISA was added by Title VI, Sec. 601(2) of P.L. 105-272, on October 20, 1998, 112 Stat. 2405-2410., and amended by P.L. 107-56 and by P.L. 107-108.

⁸³The italicized language was added by P.L. 107-56, Section 214(a)(1), replacing language which had read "for any investigation to gather foreign intelligence information or information concerning international terrorism."

⁸⁴50 U.S.C. § 1842(a)(2).

Each such application is made in writing upon oath or affirmation to a FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant orders approving installation of pen registers or trap and trace devices on behalf of a FISC judge. The application must be approved by the Attorney General or a designated attorney for the Government. Each application must identify the federal officer seeking to use the pen register or trap and trace device sought in the application. It must also include a certification by the applicant *"that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."*⁸⁵

Under 50 U.S.C. § 1842, as amended by P.L. 107-56, pen registers and trap and trace devices may now be installed and used not only to track telephone calls, but also other forms of electronic communication such as e-mail. Once an application is made under Section 1842, the judge⁸⁶ must enter an ex parte order⁸⁷ as requested or as

⁸⁵This language, added by P.L. 107-56, Section 214(a)(2), replaced stricken language which read:

(2) a certification by the applicant that the information to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General; and

(3) information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with--

(A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or

(B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

⁸⁶This section refers simply to "judge." In light of 50 U.S.C. § 1842(b), it would appear that this may refer to either a FISC judge or a U.S. magistrate judge designated by the Chief Justice under Section 1842(b)(2) to hear applications for and grant orders approving installation and use of pen registers or trap and trace devices on behalf of a FISC judge. The legislative history on this provision does not appear to clarify this point. The language was included in the bill reported out as an original measure by the Senate Select Committee on Intelligence, S. 2052, as Sec. 601. The Committee's report, S. Rept. 105-185, indicates that magistrate judges were included in the legislation to parallel their use in connection with receipt of applications and approval of pen registers and trap and trace devices in the context of criminal investigations, but reflected the Committee's understanding that the authority provided in the legislation to designate magistrate judges to consider applications for pen registers and trap and trace devices in the foreign intelligence gathering context would be closely monitored by the Department of Justice and this designation authority would not be exercised until the Committee was briefed on the compelling need for such designations,

(continued...)

⁸⁶(...continued)

as reflected, for example, through statistical information on the frequency of applications to the FISC under the new procedure. S. Rept. 105-185, at 28 (May 7, 1998). The provision creating on pen registers and trap and trace devices in foreign intelligence and international terrorism investigations, Sec. 601 of the bill as passed, was among those included in the conference version of H.R. 3694 which was passed in lieu of S. 2052. H. Conference Rept. 105-80, at 32 (October 5, 1998).

⁸⁷Under 50 U.S.C. § 1842(d)(2)(A), such an order

(A) *shall specify--*

- (i) the identity, if known, of the person who is the subject of the investigation;*
- (ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;*
- (iii) the attributes of the communications to which the order applies, such as the number or other identifies, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.*

(B) *shall direct that--*

- (i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;*
- (ii) such provider, landlord, custodian, or other person--*
 - (I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and*
 - (II) shall maintain, under security procedures approved by the Attorney General and the Director of Central Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and*
- (iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance.*

The italicized portions of this section reflect amended language from P.L. 107-56, Section 214 (a)(4).

P.L. 107-108, Section 314(a)(5)(B), replaced "of a court" at the end of 50 U.S.C. § 1842(f) with "of an order issued," so that the language now reads:

- (f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance

(continued...)

modified approving the installation and use of a pen register or trap and trace device if the application meets the requirements of that section.

Section 1843 of Title 18 of the United States Code focuses upon authorization for installation and use of a pen register or trap and trace device under FISA during specified types of emergencies. This provision applies when the Attorney General makes a reasonable determination that:

- (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain *foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of a activities protected by the first amendment to the Constitution* before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and
- (2) the factual basis for issuance of an order under section 1842(c) of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.⁸⁸

Upon making such a determination, the Attorney General may authorize the installation and use of a pen register or trap and trace device for this purpose if two criteria are met. First, the Attorney General or his designee must inform a judge referred to in Section 1842(b)⁸⁹ at the time of the emergency authorization that the decision to install and use the pen register or trap and trace device has been made. Second, an application for a court order authorizing a pen register or trap and trace device under 50 U.S.C. § 1842(a)(1) must be made to the judge as soon as practicable, but no later than 48 hours after the emergency authorization.⁹⁰ If no order approving the installation and use of a pen register or trap and trace device is forthcoming, then the installation and use of such pen register or trap and trace device must terminate at the earlier of the time when the information sought is obtained, the time when the application for the order is denied under 50 U.S.C. § 1842, or the

⁸⁷(...continued)

with the terms *of an order issued* under this section.

(Emphasis added.) Cf., 50 U.S.C. § 1805(f), which contains an immunity grant which, at first blush would appear to apply only to electronic surveillance under FISA, but which has been interpreted in H. Rept. 107-328, page 25, the conference committee accompanying H.R. 2883, which became P.L. 107-108, to apply to electronic surveillance, physical searches and pen register and trap and trace devices. See discussion at fn. 32, *supra*.

⁸⁸50 U.S.C. § 1843(b) (italics reflect language added by P.L. 107-56, § 214(b)(2), in place of language which read "foreign intelligence information or information concerning international terrorism.") Similar language was inserted in 50 U.S.C. § 1843(a) by P.L. 107-56, § 214(b)(1), in place of language that paralleled that stricken from subsection 1843(b).

⁸⁹See discussion of the term "judge" as used in Section 1842(b) in fn. 86, *supra*.

⁹⁰50 U.S.C. § 1843(a).

expiration of 48 hours from the time the Attorney General made his emergency authorization.⁹¹

If an application for an order sought under Section 1843(a)(2) is denied, or if the installation and use of the pen register or trap and trace device is terminated, and no order approving it is issued under 50 U.S.C. § 1842(b)(2), then no information obtained or evidence derived from the use of the pen register or trap and trace device may be received in evidence or disclosed in any trial, hearing or other proceeding in any court, grand jury, department, office, agency, regulatory body, legislative committee or other federal state or local authority. Furthermore, in such circumstances, no information concerning a United States person acquired from the use of the pen register or trap and trace device may later be used or disclosed in any other way by federal officers or employees without consent of the U.S. person involved, with one exception. If the Attorney General approves the disclosure because the information indicates a threat of death or serious bodily harm to anyone, then disclosure without consent of the U.S. person involved is permitted.⁹²

If Congress declares war, then, notwithstanding any other provision of law, the President, through the Attorney General, may authorize use of a pen register or trap and trace device without a court order to acquire foreign intelligence information for up to 15 calendar days after the declaration of war.⁹³

50 U.S.C. § 1845 sets parameters with respect to the use of information obtained through the use of a pen register or trap and trace device under 50 U.S.C. § 1841 *et seq.* Federal officers and employees may only use or disclose such information with respect to a U.S. person without the consent of that person in accordance with Section 1845.⁹⁴ Any disclosure by a Federal officer or employee of information acquired pursuant to FISA from a pen register or trap and trace device must be for a lawful purpose.⁹⁵ Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1841 *et seq.* is only permitted where the disclosure is accompanied by a statement that the information and any derivative information may only be used in a criminal proceeding with the advance authorization of the Attorney General.⁹⁶

Under 50 U.S.C. § 1845(c), when the United States intends to enter into evidence, use, or disclose information obtained by or derived from a FISA pen register or trap and trace device against an aggrieved person⁹⁷ in any federal trial,

⁹¹50 U.S.C. § 1843(c)(1).

⁹²50 U.S.C. § 1843(c)(2).

⁹³50 U.S.C. § 1844.

⁹⁴50 U.S.C. § 1845(a)(1).

⁹⁵50 U.S.C. § 1845(a)(2).

⁹⁶50 U.S.C. § 1845(b).

⁹⁷“Aggrieved person” is defined in 50 U.S.C. § 1841(3) for purposes of 50 U.S.C. § 1841 *et seq.* as any person:

(continued...)

hearing, or proceeding, notice requirements must be satisfied. The Government, before the trial, hearing, or proceeding or a reasonable time before the information is to be proffered, used or disclosed, must give notice of its intent both to the aggrieved person involved⁹⁸ and to the court or other authority in which the information is to be disclosed or used.

If a state or local government intends to enter into evidence, use, or disclose information obtained or derived from such a trap and trace device against an aggrieved person in a state or local trial, hearing or proceeding, it must give notice to the aggrieved person and to the Attorney General of the United States of the state or local government's intent to disclose or use the information.⁹⁹

The aggrieved person in either case may move to suppress the evidence obtained or derived from a FISA pen register or trap and trace device on one of two grounds: that the information was unlawfully acquired; or that the use of the pen register or trap and trace device was not made in conformity with an order of authorization or approval under 50 U.S.C. 1841 *et seq.*¹⁰⁰

If notice is given under 50 U.S.C. §§ 1845(c) or (d), or a motion or request is made to suppress or to discover or obtain any applications, orders, or other materials relating to use of a FISA pen register or trap and trace device or information obtained by or derived from such use, the Attorney General may have national security concerns with respect to the effect of such disclosure or of an adversary hearing. If he files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, the United States district court in which the motion or request is made, or where the motion or request is made before another authority, the U.S. district court in the same district, shall review *in camera* and *ex parte* the application, order, and other relevant materials to determine whether the use of the pen register or trap and trace device was lawfully authorized and conducted.¹⁰¹ In so doing, the court may only disclose portions of the application, order or materials to the aggrieved person or order the Attorney General to provide the aggrieved person with a summary of these materials if that disclosure is necessary to making an

⁹⁷(...continued)

(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by subchapter IV [50 U.S.C. § 1841 *et seq.*];
or
(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by subchapter IV to capture incoming electronic or other communications impulses.

⁹⁸The statute refers to notice to the "aggrieved person." Here it is using this term in the context of a pen register or trap and trace device, as defined in 50 U.S.C. § 1841(3) (see fn. 97, *supra*). This term is also defined in both 50 U.S.C. §§ 1801(k) (in the context of electronic surveillance, see fn. 35, *supra*) and 1825(d) (in the context of a physical search, see fn. 66, *supra*).

⁹⁹50 U.S.C. § 1845(d).

¹⁰⁰50 U.S.C. § 1845(e).

¹⁰¹50 U.S.C. § 1845(f)(1).

accurate determination of the legality of the use of the pen register or trap and trace device.¹⁰²

Should the court find that the pen register or trap and trace device was not lawfully authorized or conducted, it may suppress the unlawfully obtained or derived evidence or “otherwise grant the motion of the aggrieved person.”¹⁰³ On the other hand, if the court finds the pen register or trap and trace device lawfully authorized and conducted, it may deny the aggrieved person’s motion except to the extent discovery or disclosure is required by due process.¹⁰⁴ Any U.S. district court orders granting motions or request under Section 1845(g), finding unlawfully authorized or conducted the use of a pen register or trap and trace device, or requiring review or granting disclosure of applications, orders or other materials regarding installation and use of a pen register or trap and trace device are deemed final orders. They are binding on all federal and state courts except U.S. courts of appeals and the U.S. Supreme Court.¹⁰⁵

Section 1846 deals with congressional oversight of the use of FISA pen registers and trap and trace devices. It requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all FISA uses of pen registers and trap and trace devices. In addition, the Attorney General, on a semi-annual basis, must report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee on the total number of applications made for orders approving the use of such pen registers and trap and trace devices and the total number of such orders granted, modified, or denied during the previous 6 month period.

Access to certain business records for foreign intelligence purposes. Also added in 1998, Title V of FISA, 50 U.S.C. § 1861 *et seq.*, was substantially changed by P.L. 107-56 and modified further by P.L. 107-108.¹⁰⁶

¹⁰²50 U.S.C. § 1845(f)(2).

¹⁰³50 U.S.C. § 1845(g)(1).

¹⁰⁴50 U.S.C. § 1845(g)(2).

¹⁰⁵50 U.S.C. § 1845(h).

¹⁰⁶Title V of FISA was added by Title VI, Sec. 602, of P.L. 105-272, on October 20, 1998, 112 Stat. 2411-12, and significantly amended by P.L. 107-56 and P.L. 107-108. The prior version of 50 U.S.C. § 1861 provided definitions for “foreign power,” “agent of a foreign power,” “foreign intelligence information,” “international terrorism,” and “Attorney General,” “common carrier,” “physical storage facility,” “public accommodation facility,” and “vehicle rental facility” for purposes of 50 U.S.C. § 1861 *et seq.* The prior version of Section 1862 was much more narrowly drawn than the new version added in P.L. 107-56 and amended by P.L. 107-108. The earlier version read:

(a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to

(continued...)

Although denominated “access to certain business records for foreign intelligence and international terrorism investigations,” the reach of Section 1861, as amended by the

¹⁰⁶(...continued)

release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 1803(a) of this title; or
(B) a United States Magistrate Judge under chapter 43 of Title 28 [28 U.S.C. § 631 *et seq.*], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the release of records under this section on behalf of a judge of that court; and

(2) shall specify that—

(A) the records concerned are sought for an investigation described in subsection (a); and
(B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.

(c)(1) Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application satisfied the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d)(1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).

(2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility, physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of Investigation has sought or obtained records pursuant to an order under this section.

Congressional oversight was covered under the prior provisions by 50 U.S.C. §1863, which was similar, but not identical to the new Section 1862. The former Section 1863 stated:

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all request for records under this subchapter [50 U.S.C. § 1861 *et seq.*].

(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

(1) the total number of applications made for orders approving requests for records under this subchapter [50 U.S.C. § 1861 *et seq.*]; and

(2) the total number of such orders either granted, modified, or denied.

USA PATRIOT Act and P.L. 107-108, is now substantially broader than business records alone. Under 50 U.S.C. § 1861(a)(1), the Director of the FBI, or his designee (who must be at the Assistant Special Agent in Charge level or higher in rank) may apply for an order requiring

... the production of any tangible things (including books, records, papers, documents, and other items) for an investigation *to obtain foreign intelligence information not concerning a United States person* or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.¹⁰⁷

Subsection 1861(a)(2) requires that such an investigation must be conducted under guidelines approved by the Attorney General under E.O. 12333 or a successor order and prohibits such an investigation of a United States person based solely upon First Amendment protected activities.

An application for an order under Section 1861 must be made to an FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant such orders for the production of tangible things on behalf of an FISC judge.¹⁰⁸ The application must specify that the "records"¹⁰⁹ are sought for "an authorized investigation conducted in accordance with

¹⁰⁷The italicized portion of Section 1861(a)(1) was added by Section 314(a)(6) of P.L. 107-108. H. Rept. 107-328, the conference report to accompany H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), at page 24, describes the purpose of this addition as follows:

Section 215 of the USA PATRIOT Act of 2001 amended title V of the FISA, adding a new section 501 [50 U.S.C. § 1861]. Section 501(a) now authorizes the director of the FBI to apply for a court order to produce certain records "For an investigation to protect against international terrorism or clandestine intelligence activities." Section 501(b)(2) directs that the application for such records specify that the purpose of the investigation is to "obtain foreign intelligence information not concerning a United States person." However, section 501(a)(1), which generally authorizes the applications, does not contain equivalent language. Thus, subsections (a)(1) and (b)(2) now appear inconsistent.

The conferees agreed to a provision which adds the phrase "to obtain foreign intelligence information not concerning a United States person or" to section 501(a)(1). This would make the language of section 501(a)(1) consistent with the legislative history of section 215 of the USA PATRIOT Act (*see* 147 Cong. Res. S11006 (daily ed. Oct. 25, 2001) (sectional analysis)) and with the language of section 214 of the USA PATRIOT Act (authorizing an application for an order to use pen registers and trap and trace devices to "obtain foreign intelligence information not concerning a United States person.").

¹⁰⁸50 U.S.C. § 1861(b)(1).

¹⁰⁹While the language refers to "records," it is worthy of note that the authority conferred upon the Director of the FBI or his designee under Section 1861(a) encompasses applications for orders requiring production of "any tangible thing (including books, (continued...)

[50 U.S.C. § 1862(a)(2)] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.”¹¹⁰ When such an application is made, the judge must enter an *ex parte* order “as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.”¹¹¹ Such an order shall not disclose that it is issued for purposes of an investigation under 50 U.S.C. § 1861(a).¹¹² Subsection 1861(d) prohibits any person to disclose that the FBI has sought or obtained tangible things under Section 1861, except where the disclosure is made to persons necessary to the production of tangible things involved. Subsection 1861(e) precludes liability for persons who, in good faith, produce tangible things under such a Section 1861 order. It further indicates that production does not constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1862 deals with congressional oversight. Subsection 1862(a) requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all request for production of tangible things under Section 1861.¹¹³ Subsection 1862(b) requires the Attorney General to report to the House and Senate Judiciary Committees on the total number of applications for Section 1861 orders for production of tangible things and on the total number of such orders granted, modified, or denied during the previous 6 months.

New Private Right of Action

In addition to provisions which amended FISA explicitly, other provisions of the USA PATRIOT Act touched upon FISA, at least tangentially. For example, Section 223 of the Act, among other things, created a new 18 U.S.C. § 2712. This new section, in part, created an exclusive private right of action for any person aggrieved by any willful violation of sections 106(a), 305(a), or 405(a) of FISA (50 U.S.C. §§ 1806(a), 1825(a), 1845(a), respectively) to be brought against the United States in U.S. district court to recover money damages. Such monetary relief would amount

¹⁰⁹(...continued)

records, papers, documents, and other items.” One might argue, therefore, that for Subsection 1861(a)(1) and Subsection 1861(b)(2) to be read in harmony, a court might interpret “records” more broadly to cover “any tangible thing.” On the other hand, if, by virtue of the specific reference in Subsection 1861(a)(1) to “records” as only one of many types of “tangible things,” the term “records” in Subsection 1861(b)(2) were to be read narrowly, it might lead to some confusion as to the nature and scope of any specification that might be required where an application seeking production of types of tangible things other than records is involved.

¹¹⁰50 U.S.C. § 1861(b)(2).

¹¹¹50 U.S.C. § 1861(c)(1).

¹¹²50 U.S.C. § 1861(c)(2).

¹¹³Section 314(a)(7) of P.L. 107-108 corrected two references in 50 U.S.C. § 1862 as passed in the USA PATRIOT Act. P.L. 107-108 replaced “section 1842 of this title” with “section 1861 of this title,” in both places in 50 U.S.C. § 1862 where it appeared.

to either actual damages or \$10,000, whichever is greater; and reasonably incurred litigation costs. It also set forth applicable procedures.¹¹⁴

USA PATRIOT Act Sunset Provision

Section 224 of the USA PATRIOT Act set a sunset for many of the provisions in the Act of December 31, 2005. Among those provisions which will sunset pursuant to this are all of the amendments to FISA, and subsequent amendments thereto, except the provision which increased the number of FISC judges from 7 to 11 (Section 208 of P.L. 107-56). Section 224 also excepts from the application of the sunset provision any particular foreign intelligence investigations that began before December 31, 2005, or any particular offenses or potential offenses which began or occurred before December 31, 2005. As to those particular investigations or offenses, applicable provisions would continue in effect.

Conclusion

The Foreign Intelligence Surveillance Act, as amended, provides a statutory structure to be followed where electronic surveillance, 50 U.S.C. § 1801 *et seq.*, physical searches, 50 U.S.C. § 1821 *et seq.*, or pen registers or trap and trace devices, 50 U.S.C. § 1841 *et seq.*, for foreign intelligence gathering purposes are contemplated. It creates enhanced procedural protections where a United States person is involved, while setting somewhat less stringent standards where the surveillance involves foreign powers or agents of foreign powers. With its detailed statutory structure, it appears intended to protect personal liberties safeguarded by the First and Fourth Amendments while providing a means to ensure national security interests.

The USA PATRIOT Act, P.L. 107-56, increased the number of FISC judges from 7 to 11, while expanding the availability of FISA electronic surveillance, physical searches and pen registers and trap and trace devices. For example, under P.L. 107-56, an application for a court order permitting electronic surveillance or a physical search under FISA is now permissible where “a significant” purpose of the surveillance or physical search, rather than “the” purpose or, as interpreted by some courts, the primary purpose of the surveillance is to gather foreign intelligence information. While the previous language withstood constitutional challenge, the

¹¹⁴Another provision, Section 901 of the USA PATRIOT Act, amended 50 U.S.C. § 403-3(c) (Section 103(c) of the National Security Act of 1947) regarding the responsibilities of the Director of Central Intelligence (DCI). The amendment added to those authorities and responsibilities, placing upon the DCI the responsibility for the establishment of

. . . requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 *et seq.*), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that Act unless otherwise authorized by statute or Executive order.

constitutional sufficiency of the change in the FISA procedures under the Fourth Amendment is, as yet, untested.

The USA PATRIOT Act also amended FISA to allow court orders permitting so-called multipoint or “roving” electronic surveillance, where the orders do not require particularity with respect to the identification of the instrument, place, or facility to be intercepted, upon a finding by the court that the actions of the target of the surveillance are likely to thwart such identification. P.L. 107-108 further clarified this authority.

Under the Act, pen registers and trap and trace devices may now be authorized for e-mails as well as telephone conversations. In addition, the Act expanded the previous FBI access to business records, permitting court ordered access in connection with a foreign intelligence or international terrorism investigation not just to business records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities, but to any tangible things.

While expanding the authorities available for foreign intelligence investigations, FISA, as amended by the USA PATRIOT Act and the Intelligence Authorization Act for FY 2002, also contains broader protections for those who may be the target of the various investigative techniques involved. For example, whether the circumstances involve electronic surveillance, physical searches, pen registers or trap and trace devices or access to business records and other tangible items, FISA, as amended by the USA PATRIOT Act, does not permit the court to grant orders based solely upon a United States person’s exercise of First Amendment rights.¹¹⁵

In addition, P.L. 107-56 created a new private right of action for persons aggrieved by inappropriate disclosure or use of information gleaned or derived from electronic surveillance, physical searches or the use of pen registers or trap and trace devices. These claims can be brought against the United States for certain willful violations by government personnel.

Finally, the inclusion of a sunset provision for the FISA changes made in the USA PATRIOT Act, with the exception of the increase in the number of FISC judges, provides an opportunity for the new authorities to be utilized and considered, and an opportunity for the Congress to revisit them in light of that experience.

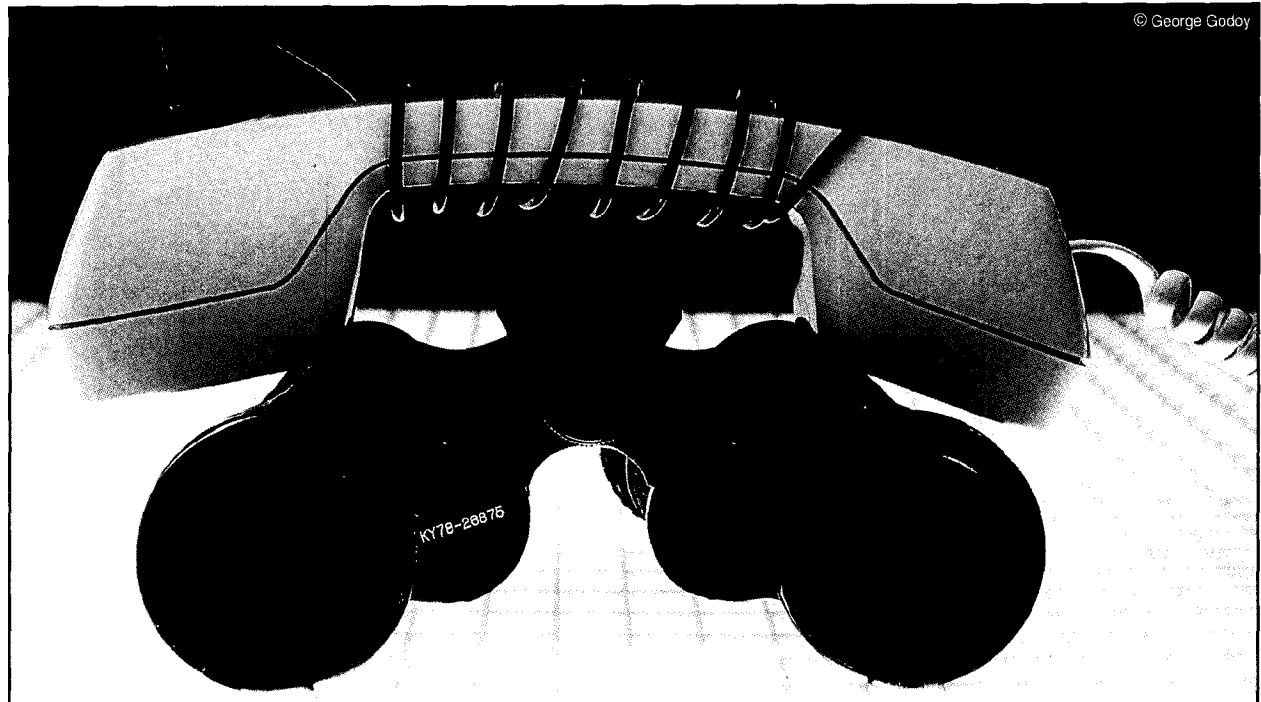
¹¹⁵See, e.g., 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A), 1842(a)(1), 1843(b), 1861(a)(1), and 1861(a)(2).

Foreign Intelligence Surveillance Act

Before and After the USA PATRIOT Act

By MICHAEL J. BULZOMI, J.D.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-16-2005 BY 65179/DMH/LP/RW 05-cv-0845



© George Godoy

The terrorist attacks of September 11, 2001, left an indelible mark upon America and an overshadowing feeling of vulnerability. They also created a determination to respond to the new national security threats they represented. Congress reacted to these threats by passing laws providing new tools to fight terrorism. Perhaps, the most controversial recent act of Congress is the United and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

Act of 2001¹ (USA PATRIOT Act) and its impact upon the use of electronic surveillance and physical searches authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)² to combat foreign threats.

Some Americans fear the actions taken by Congress may infringe upon basic American liberties. Benjamin Franklin warned that "those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety."³ The government must

use its new tools in a way that preserves the rights and freedoms guaranteed by America's democracy, but, at the same time, ensure that the fight against terrorism is vigorous and effective. No American should be forced to seek safety over liberty. This article briefly examines FISA and the impact of the USA PATRIOT Act upon it.

FISA

Electronic monitoring (including both wiretaps and microphone installations) and physical searches

are excellent, and sometimes essential, sources of information for both foreign intelligence and criminal activities. In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act. Title III of that act⁴ contains provisions concerning the authorization and use of electronic monitoring by the government to gather information regarding criminal activities. Under Title III, the government has specific authorization procedures and rules to follow when it monitors people and places to collect evidence of violations of criminal laws. But, Title III did not answer the question of whether or not the government is required to obtain court authorization for electronic monitoring conducted, not for criminal investigations but for the collection of information regarding threats to national security.

The U.S. Supreme Court faced this issue in the case of *United States v. United States District Court*.⁵ In this case, a group of Vietnam War protesters tried to

blow up the local CIA recruiting office in Ann Arbor, Michigan, and a number of other government buildings. Evidence obtained during a domestic national security wire interception, undertaken without a formal court order, was used in the subsequent criminal trial. The use of this evidence was contested. The issue was whether or not the president had the authority, through the attorney general, to authorize electronic surveillance for national security matters without prior judicial review. The Court held that the government does not have unlimited power to conduct national security wiretaps for domestic security matters, and that prior judicial authorization is needed before using wiretaps for national security purposes. However, the Court recognized that such wiretaps involve different policy and practical considerations from ordinary criminal wiretaps. It suggested that Congress consider exploring the issue and decide if the authorization for and

rules governing the use of national security wiretaps should be the same as those governing criminal wiretaps. The Court made it clear that it was not deciding the issue of the government's authority to conduct wiretaps in cases of foreign threats to the national security.

To establish the necessary authority and procedures for the government to conduct wiretaps in response to foreign threats, Congress passed FISA. FISA established a requirement of judicial approval before the government engages in an electronic surveillance (as well as physical searches) for foreign intelligence purposes. The act established the FISA Court, consisting of U.S. District Court judges designated by the chief justice of the U.S. Supreme Court. The court's purpose is to review government applications for national security electronic monitoring and searches and authorize their use with appropriate limitations. If the FISA Court denies an application for an order authorizing a national security wiretap or search, the matter is referred under seal to the FISA Court of Review, comprised of three federal judges selected by the chief justice of the U.S. Supreme Court. The court of review determines whether the application was properly denied.⁶ Its decision can be appealed directly to the U.S. Supreme Court.

FISA Contrasted with Title III

In essence, the purpose of a FISA order is to gather foreign intelligence information,⁷ while the purpose of a Title III wiretap order is to gather evidence for criminal prosecution. The FISA application



Special Agent Bulzoni is a legal instructor at the FBI Academy.

“The government must use its new tools in a way that preserves the rights and freedoms guaranteed by America’s democracy, but, at the same time, ensure that the fight against terrorism is vigorous and effective.”

need only state facts supporting probable cause to believe that the target of the intercept (or search) is a foreign power, or an agent of a foreign power, and that the facilities to be monitored or searched are being used, or are about to be used, by a foreign power, or an agent of a foreign power, and to certify that a significant purpose of the surveillance is to obtain foreign intelligence information.⁸ To show that a person is an agent of a foreign power, the government need only relate facts demonstrating that the subject is an officer or employee of a foreign power or acts on the foreign power's behalf; or knowingly engages in clandestine intelligence-gathering activities that may involve a violation of U.S. criminal statutes; or knowingly engages in sabotage, international terrorism, or in the preparation of these activities on behalf of a foreign power.⁹

In contrast, a criminal Title III wiretap must be supported by probable cause to believe that a specific individual, using an identified phone or location, is committing a particular crime.¹⁰ It requires that the government show that a predicate offense is, has, or will be committed by the subject of the surveillance¹¹ and that particular communications concerning the predicate offense will be obtained through the wiretap¹² at a specified location or through a specified device used by the target.¹³

FISA Information for Criminal Prosecutions

It is important to note that both FISA and Title III require a showing of probable cause to authorize electronic monitoring (and physical

searches in the case of FISA). However, because of the differing objectives of the two acts, the degree of specificity required differs markedly. Arguably, because of the different probable cause showing required by FISA, it is easier for the government to obtain a FISA order than it is to obtain a Title III order. Because of this, the courts became concerned that the government

“

...both FISA and Title III require a showing of probable cause to authorize electronic monitoring (and physical searches in the case of FISA).

”

would obtain FISA electronic surveillance orders in what were essentially criminal investigations to avoid the stricter requirements of Title III.

This concern surfaced in an espionage case that predates FISA. In *United States v. Truong Dinh Hung*,¹⁴ the government used a warrantless wiretap to overhear and record telephone conversations of the defendant and to bug his apartment. The wiretapping and bugging were authorized by the attorney general under the “foreign intelligence” exception to the Fourth Amendment. The defendant moved to suppress the evidence collected by means of the wiretap and bug as

violations of the Fourth Amendment. The U.S. Court of Appeals for the Fourth Circuit admitted the evidence collected during the early days of the collection but held that evidence obtained after the primary purpose of the investigation had shifted from securing intelligence information to accumulating evidence of a crime and must be suppressed because of the failure to comply with the requirements of Title III. This ruling is the origin of the “primary purpose” test that was to create problems in later cases.

Subsequent cases decided after the passage of FISA distinguished *Truong* on the grounds that the surveillance authorization in that case was not obtained pursuant to a FISA warrant.¹⁵ These courts noted that FISA contains a statutory mechanism for the dissemination of criminal information obtained during an intelligence intercept and have held that when such evidence is discovered “incidentally” during an authorized FISA intercept it may be admitted in subsequent criminal prosecutions.¹⁶ This would include situations where “the government can anticipate that the fruits of such surveillance may later be used, as allowed by [the statute], as evidence in a criminal trial.”¹⁷ This line of reasoning became known as the “primary purpose” test and was adopted by several circuits.¹⁸ In other words, when the primary object of the electronic monitoring (or search) was to collect foreign intelligence information, FISA was the appropriate mechanism to seek authorization from the courts. When the primary purpose was to seek criminal prosecution, Title III was the appropriate mechanism. Failure

to strictly observe this distinction resulted in a possible suppression of the evidence.

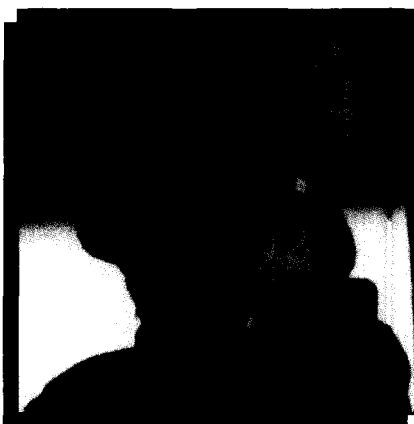
The "primary purpose" test led the FISA Court and the U.S. Department of Justice (DOJ) to adopt a policy of building a "wall" between intelligence investigators and criminal investigators for fear of tainting FISA court ordered surveillances. Intelligence investigators were not to discuss ongoing foreign intelligence or foreign counterintelligence investigations with criminal investigators. In this way, FISA orders could not be used by criminal investigators to avoid seeking Title III orders. This practice led to a critical lack of coordination in investigations, such as international terrorism cases, which have both intelligence and criminal aspects.

FISA AS AMENDED BY THE USA PATRIOT ACT

Following the September 11, 2001, terrorist attacks, Congress reassessed intelligence-gathering procedures and passed the USA PATRIOT Act. The most significant changes involve the purposes for which FISA-authorized electronic monitoring and searches may be used and the exchange of information between criminal and foreign intelligence investigators.

Previously, FISA-authorized electronic monitoring and searches only could be used if high-level executive officials certified that "the purpose" was to obtain foreign intelligence information. As noted, that language came to be interpreted as the "primary purpose" by the courts and DOJ. The USA PATRIOT Act now requires that foreign intelligence information

gathering be a "significant purpose."¹⁹ The act amends FISA so that intelligence officials may coordinate efforts with law enforcement officials to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities without undermining the required certification of the "significant purpose" of FISA orders. The result is that Congress rejected the idea of having a "wall" between foreign intelligence and law enforcement officials when the object of the investigation is to detect, prevent, or prosecute foreign intelligence crimes.



On March 6, 2002, Attorney General John D. Ashcroft implemented the USA PATRIOT Act by establishing a new DOJ policy regarding information-sharing procedures. The new procedures permitted the complete exchange of information and advice between intelligence officers and law enforcement officers regarding FISA surveillances and searches.

On May 17, 2002, the FISA Court rejected the attorney general's new policy.²⁰ The FISA Court

ruled that law enforcement officials cannot a) direct or control an investigation using FISA searches or surveillances for law enforcement objectives, b) direct or control the use of FISA procedures to enhance a criminal prosecution, c) make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances, or d) that representatives of DOJ's Office of Intelligence Policy and Review (OIPR) be invited to ("chaperone" in the view of the DOJ) all meetings between FBI and DOJ's Criminal Division to consult regarding efforts to investigate or protect against foreign attack, sabotage, or international terrorism to ensure that foreign intelligence gathering remains the primary purpose of any FISA-authorized technique. The FISA Court's rejection of the new guidelines led to the first-ever appeal to the FISA Court of Review.

In its decision, the FISA Court of Review decided that FISA does not preclude or limit the government's use of foreign intelligence information, including evidence of crimes, in certain types of criminal prosecutions.²¹ The court of review determined that the restrictions imposed by the FISA Court on the government are not required by FISA, as amended by the USA PATRIOT Act or by the Constitution and that the USA PATRIOT Act amendments of the FISA statute do not violate the Fourth Amendment of the Constitution.

The court of review made several important points. First, there must be a significant foreign intelligence information-gathering

purpose for every FISA application for electronic monitoring or search, such as recruiting a foreign spy as a double agent, identification of foreign intelligence taskings, or the discovery of foreign spy tradecraft.²²

Second, the court determined that FISA could be used to obtain evidence primarily for a criminal prosecution if the prosecution is an offense related to a foreign intelligence threat (a foreign intelligence crime) and a significant foreign intelligence-gathering purpose also is present.²³ The court defined foreign intelligence crimes as those listed in the FISA statute, including espionage, international terrorism, unlawful clandestine intelligence activities, sabotage, identity fraud offenses committed for or on behalf of a foreign power, and aiding or abetting or conspiring to commit these offenses.²⁴ Additionally, any ordinary crime intertwined with a foreign intelligence activity is included, such as bank robbery to finance terrorist actions or even credit card fraud to hide the identity of a spy.²⁵

Finally, the court recognized that the USA PATRIOT Act lawfully breached the "wall" between criminal law enforcement and intelligence or counterintelligence gathering. Congress' intent in this matter is demonstrated amply by its addition of a new section to FISA by the USA PATRIOT Act. The new FISA Section 1806(k) reads:

- 1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with federal law enforcement officers to

coordinate efforts to investigate or protect against

- a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
- b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

**“
...additional
safeguards are built
into FISA if the target
of the monitoring
or search is a U.S.
citizen or an alien
admitted for
permanent residence.
”**

- 2) Coordination authorized under paragraph 1 shall not preclude the certification required by Section [1804](a)(7)(B) of this title or the entry of an order under Section [1805] of this title.²⁶

This decision by the FISA Court of Review vindicates Congress' and the attorney general's view of FISA. It is permissible for intelligence and law enforcement officials to coordinate their efforts

using all available resources, including FISA surveillances and searches, to detect, frustrate, and convict spies and terrorists.

It is important to note that additional safeguards are built into FISA if the target of the monitoring or search is a U.S. citizen or an alien admitted for permanent residence. The burden placed upon the government to obtain a FISA order is higher if the target is a U.S. person.²⁷ The act clearly states that the simple exercise of First Amendment rights by U.S. persons cannot be the basis for considering that person to be an agent of a foreign power.²⁸ The act also clearly establishes how and when information regarding a U.S. person may be used.²⁹

USA PATRIOT Act and Information Sharing

An extremely important aspect of the USA PATRIOT Act is that it permits greater sharing of intelligence information between law enforcement and national security investigators, regardless of the source of the intelligence information. Section 203 of the USA PATRIOT Act amends Rule 6 of the Federal Rules of Criminal Procedure to permit the disclosure of grand jury information containing foreign intelligence information to "any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties."³⁰ The reporting requirement differs in that the name of the individual receiving the information is not given to the court, only

the department or agency receiving the information. This section also amends Title III (the federal wiretap statute) to permit the same type of disclosure of intelligence information gathered during a court authorized criminal wiretap.³¹

Section 905 of the act³² underscores the importance that Congress assigns to information sharing. That section requires the attorney general, or any head of a federal department or agency with law enforcement responsibility, to promptly disclose to the director of the CIA any foreign intelligence information gathered as a result of a criminal investigation.

Other Related Amendments

The USA PATRIOT Act amended many federal statutes in significant ways that are important to criminal and intelligence investigators. It is impossible to discuss all of these amendments in this limited space. However, some of these amendments should be mentioned.

A very significant change is that the USA PATRIOT Act makes terrorism a predicate offense allowing for a wiretap under Title III.³³ Investigators now have a choice, depending on the nature of the investigation, to apply for a FISA order or a Title III wiretap order.

In addition, the act also allows for a roving wiretap under FISA.³⁴ Roving wiretaps allow law enforcement to respond to time-sensitive criminal or terrorist activity by continuing court sanctioned electronic surveillance, even if the target of the surveillance rapidly switches cellular telephones, Internet accounts, or meeting venues.

USA PATRIOT Act and Pen Registers and Traps and Traces

FISA contains specific provisions regarding the use of pen registers and traps and traces in foreign intelligence investigations.³⁵ Section 214 of the USA PATRIOT Act changes the standard for issuing pen registers and trap and trace orders. FISA pen registers and traps and traces now can be obtained when the government certifies that the information likely to be obtained is foreign intelligence information

“
...the USA PATRIOT Act makes terrorism a predicate offense allowing for a wiretap under Title III.
”

not concerning a U.S. person or is relevant to ongoing investigations to protect against terrorism or clandestine intelligence activities.³⁶ Prior to the USA PATRIOT Act, pen register and trap and trace orders required showing that there was relevance to an investigation and that there was reason to believe that the targeted line was being used by an agent of a foreign power or someone in communication with such an agent under certain circumstances. The second requirement no longer exists.

The USA PATRIOT Act also amended Title III, FISA, and the federal statute related to pen registers to explicitly authorize the use of pen registers and traps and traces

on communication networks other than just telephones.³⁷ Computer networks and cellular telephones are now specifically subject to this technique.

Criminal pen register and trap and trace orders are no longer limited to the geographic area within the jurisdiction of the issuing court.³⁸ All service providers necessary to the execution of the order, regardless of their location, are covered by such orders.

USA PATRIOT Act and Physical Searches

Historically, some federal courts permitted the government to search premises, but delay for a reasonable time the required notice that the government had entered the premises.³⁹ The USA PATRIOT Act amended federal law to statutorily recognize the practice.⁴⁰ Delayed notice, or sneak-and-peek warrants, are now permissible where the court finds reasonable cause to believe that immediate notification of the execution of the warrant would have an adverse result.⁴¹ The warrant must prohibit the seizure of tangible property unless the court finds it necessary. The warrant also must provide for giving notice of the search within a reasonable time, but extensions of time can be granted.

The act expands the reach of search warrants in domestic and international terrorism cases.⁴² Ordinarily, criminal search warrants must be issued in the districts where the searches will occur.⁴³ Under the new rule, however, a magistrate judge in a district “in which activities related to the terrorism may have occurred”⁴⁴ may issue a war-

rant in that terrorism investigation that can be executed within or outside that district.

It is important to note that there is a 4-year sunset provision for some parts of the act.⁴⁵ The sharing of grand jury information portion of the act does not expire as of December 31, 2005. However, the "significant purpose" certification for FISA intercepts, the provisions regarding roving FISA surveillance, and the pen register and trap and trace do.

CONCLUSION

From a national security and law enforcement perspective, the United States has made considerable progress through recent court cases and congressional action toward ensuring that threats to national security are effectively investigated and countered. At the same time, care must be taken to ensure that the new tools provided by Congress in the USA PATRIOT Act are employed within the constraints of the Constitution. The Supreme Court has said "the police must obey the law while enforcing the law, that in the end life and liberty can be as much endangered from illegal methods used to convict those thought to be criminals as from the actual criminals themselves."⁴⁶

FISA's different standards for intelligence surveillance have been viewed suspiciously by some who fear the loss of individual liberty. Care must be taken to avoid any abuse of this tool by law enforcement. The Court has warned that "the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but

without understanding."⁴⁷ Government should not overstep its bounds.

Law enforcement must act aggressively to investigate and prevent attacks from those who wish this country harm. At the same time, there must be oversight, both internal and external, to ensure that law enforcement is not overzealous. FISA and the USA PATRIOT Act provide such oversight. While the USA PATRIOT Act removed many of the obstacles that hindered terrorist and intelligence investigations in the past, it did not give law enforcement and intelligence agencies a free hand. The actions of

© K. L. Morrison



the government still are conducted under the watchful eye of the courts. In the end, law enforcement and intelligence investigators must be mindful that the constitutional protections that limit their authority also serve to protect their own rights as citizens of the United States. ♦

Endnotes

¹ PL 107-56, October 26, 2001, 115 Stat 272.

² 50 U.S.C. §§ 1801-1863(1994).

³ Reply of the Pennsylvania Assembly to the governor, November 11, 1775.

⁴ 18 U.S.C. §§ 2510-2520.

⁵ 407 U.S. 297 (1972).

⁶ 50 U.S.C. § 1803(b).

⁷ 50 U.S.C. § 1804(a)(7)(B). Foreign intelligence information is defined as "(1) information that relates to, and if concerning a U.S. person is necessary to, the ability of the United States to protect against (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to (a) the national defense or the security of the United States; or (b) the conduct of the foreign affairs of the United States." See 50 U.S.C. § 1801 (e).

⁸ 50 U.S.C. § 1804.

⁹ 50 U.S.C. § 1801 (b).

¹⁰ 18 U.S.C. § 2518(3).

¹¹ 18 U.S.C. § 2518(3)(a).

¹² 18 U.S.C. § 2518(3)(b).

¹³ 18 U.S.C. § 2518(3)(d).

¹⁴ 629 F.2d 908 (4th Cir. 1980).

¹⁵ *United States v. Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

¹⁶ *United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987), and *United States v. Duggan*, 743 F.2d 59, 73 n.5 (2d Cir. 1984).

¹⁷ *United States v. Duggan*, 743 F.2d 59, at 78 (2d Cir. 1984) and *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987).

¹⁸ *United States v. Megahey*, 553 F.Supp. 1180 (E.D.N.Y. 1982) *aff'd sub nom. United States v. Duggan*, 743 F.2d 59 (2nd Cir. 1984); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987); *United States v. Badia*, 827 F.2d 1458 (11th Cir.1987), *cert. denied* 485 U.S. 937 (1988); *United States v. Johnson*, 952 F.2d 565 (1st Cir. 1991), *cert. denied* 506 U.S. 816 (1992).

¹⁹ PL 107-56, October 26, 2001, 115 Stat 272, § 218 (amending 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)).

²⁰ *In re All matters Submitted to Foreign Intelligence Surveillance Court*, 218 F.Supp. 611.

²¹ *In re Sealed Case*, 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev., 2002).

²² *Id.* at 736.

²³ *Supra* note 21 at 743.

²⁴ *Supra* note 21 at 723; 50 U.S.C. § 1801(a)-(c).

²⁵ *Supra* note 21 at 736.

²⁶ *Supra* note 21 at 733; 50 U.S.C. § 1806(k).

²⁷ 50 U.S.C. § 1801(b) distinguishing between agents of a foreign power who are U.S. persons and non-U.S. persons and setting out a somewhat higher standard for a U.S. person to be considered an agent of a foreign power; § 1801(e) setting out a stricter definition of foreign intelligence information where U.S. persons are involved.

²⁸ 50 U.S.C. § 1805(a)(3)(A); § 1824(a)(3)(A); § 1842(c)(2).

²⁹ 50 U.S.C. § 1801(h); § 1805(f); § 1806(a),(j); § 1821(4); § 1824(e)(4); § 1825; § 1843(c)(2); § 1845.

³⁰ *Supra* note 1, § 203a, amending Rule 6(e)(3)(c)(I)(V).

³¹ *Supra* note 1, § 203b.

³² *Supra* note 1, § 905.

³³ *Supra* note 1, § 201, amending 18 U.S.C. 2516(1).

³⁴ *Supra* note 1, § 206, amending 50 U.S.C. § 1805(c)(2)(B).

³⁵ 50 U.S.C. §§ 1841-1846.

³⁶ *Supra* note 1, § 214, amending 50 U.S.C. § 1842(c)(2).

³⁷ *Supra* note 1, §§ 214 and 216 (amending 50 U.S.C. §§ 1842, 1843, and 18 U.S.C. §§ 3121, 3123, and 3127).

³⁸ *Supra* note 1, § 216 (amending 18 § 3123; 3123(b)(1)(C) no longer requires that geographic limits be specified; however, 3127(2)(A) imposes a "nexus").

³⁹ *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986); *United States v. Ludwig*, 902 F.Supp. 121 (W.D. Tex. 1995); *United States v. Villegas*, 899 F.2d 1324 (2nd Cir.1990); *United States v. Pangburn*, 983 F.2d 449 (2nd Cir. 1993).

⁴⁰ *Supra* note 1, § 213, amending 18 U.S.C. § 3103a.

⁴¹ Adverse result is defined as one resulting in endangering a life or a person's physical safety; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; serious jeopardy of an

investigation or undue delay in trial; see 18 U.S.C. § 2705(a)(2).

⁴² *Supra* note 1, § 219, amending F.R.C.P. Rule 41(b)(3). International terrorism is defined in Title 18 U.S.C. § 2331(1); domestic terrorism is defined in 18 U.S.C. § 2331(5).

⁴³ There is an exception to this rule for movable objects; see F.R.C.P. Rule 41(b)(2).

⁴⁴ *Supra* note 42.

⁴⁵ *Supra* note 1, § 224(a).

⁴⁶ *Spano v. New York*, 79 S. Ct. at 1206 (1959).

⁴⁷ *Olmstead v. United States*, 48 S. Ct. 564 at 572-573 (1928).

Law enforcement officers of other than federal jurisdiction who are interested in this article should consult their legal advisors. Some police procedures ruled permissible under federal constitutional law are of questionable legality under state law or are not permitted at all.

Subscribe Now



United States Government INFORMATION

Order Processing Code:

* 5902

☐ YES, please send _____ subscriptions to:
FBI Law Enforcement Bulletin

The total cost of my order is \$ _____.

Name or title (Please type or print)

Company name Room, floor, suite

Street address

City State Zip code+4

Daytime phone including area code

Purchase order number (optional)

Credit card orders are welcome!

Fax orders: (202) 512-2250

Phone orders: (202) 512-1800

Online orders: bookstore.gpo.gov

(FBIEB) at \$36 each (\$45 foreign) per year.

Price includes regular shipping & handling and is subject to change.

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐

☐ VISA ☐ MasterCard ☐ Discover

☐

(expiration date)

☐

Authorizing signature

1/2001

Mail to: Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Important: Please include this completed order form with your remittance.

Thank you for your order!

~~SECRET~~

~~Secret~~ (by ~~57~~ 57-03 E-mail)

Memorandum



To :
Assistant Attorney General
Office of Legal Policy
Department of Justice

From :
Associate General Counsel
Office of the General Counsel

Subject : Library Usage

Date 04/29/2003

b6
b7C

DATE: 12-16-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-16-2030

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b5

ep. Dir. _____
Chief of Staff _____
Att. of Gen. _____
Counsel _____
Asst. Dir.: _____
Admin. Ser. _____
Crim. Inv. _____
CJIS _____
Finance _____
Info. Res. _____
Lab. _____
National Sec. _____
OPR _____
Off. of Public _____
& Cong. Affs. _____
Training _____
Off. of EEOA _____
Director's Office _____

J. Patrick Rowan
C. Steele

(PENTTBOMB UNIT)

b6
b7C

~~Secret~~
~~SECRET~~

MAIL ROOM ☐

FBI/DOJ

~~SECRET~~

b6
b7C

Memorandum from [redacted]
Re: Library Usage, 04/29/2003

Classified
~~*Secret*~~

(S)

b1
b2
b6
b7C
b5

If I can assist you in any other way, please contact me
at [redacted] or Assistant General Counsel [redacted]
[redacted]

~~Secret~~

~~SECRET~~

CRS Report for Congress

Received through the CRS Web

Proposed Change to the Foreign Intelligence Surveillance Act (FISA) under S. 113

Jennifer Elsea
Legislative Attorney
American Law Division

Summary

The Senate recently passed S. 113, a bill in the 108th Congress to extend the coverage of the Foreign Intelligence Surveillance Act ("FISA") to non-United States persons who engage in international terrorism or activities in preparation for international terrorism, without a showing of membership in or affiliation with an international terrorist group. FISA provides a means by which the government can obtain approval to conduct electronic surveillance (wiretap) and other searches with respect to a foreign power or its agents in order to obtain intelligence related to espionage, terrorism, or other matters involving national security.

The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, provides a framework for the use of electronic surveillance and other investigative methods to acquire foreign intelligence information. This measure seeks to strike a balance between national security needs in the context of foreign intelligence gathering and privacy rights guaranteed by the Fourth Amendment of the Constitution.¹ FISA provides a means by which the government can obtain approval to conduct searches and surveillance of a foreign power or its agents without first meeting the more stringent standard in Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.* [hereinafter "Title III"] that applies to criminal investigations. While Title III requires a showing of probable cause that a proposed target has committed, is committing, or is about to commit a crime, FISA requires a showing of probable cause to believe that the target is a foreign power or an agent of a foreign power.

¹ U.S. CONST. Amend. IV provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In the aftermath of the September 11, 2001 terrorist attacks on the United States, Congress amended FISA so that it no longer requires a certification that the (primary) purpose of a search or surveillance is to gather foreign intelligence information.² As amended by the USA PATRIOT Act,³ FISA requires that a “significant purpose” of the investigation be the collection of foreign intelligence information, which has been interpreted to expand the types of investigations that may be permitted to include those in which the primary purpose may be to investigate criminal activity, as long as there is at least a measurable purpose related to foreign intelligence gathering.⁴ The proposed change under S. 113 would remove the requirement for the government to show that the intended target is associated with a foreign power, as long as the intended target is not a U.S. person.

The bill was introduced in the 107th Congress as S. 2586 (known as the Schumer-Kyl Bill). In its original form, it would have amended the definition of “foreign power”⁵ to include (4) *any person, other than a United States person, or group that is engaged in international terrorism or activities in preparation therefor* [proposed new language in S. 2586 emphasized]. The Senate Select Committee on Intelligence held hearings on the bill on July 31, 2002,⁶ but the bill never reached a floor vote. Re-introduced in the 108th Congress as S. 113, the bill was amended in committee to retain the existing definition of “foreign power,” but to add a new subparagraph (c) to the definition of “agent of a

² See CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance*. “Foreign Intelligence Information” is defined in 50 U.S.C. § 1801(e) to mean:

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —
 - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
 - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —
 - (A) the national defense or the security of the United States; or
 - (B) the conduct of the foreign affairs of the United States.

³ P.L. 107-56 § 218.

⁴ See *In re Sealed Case*, 310 F.3d 717, 735 (F.I.S.Ct.Rev. 2002) (“The addition of the word “significant” to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.”).

⁵ “Foreign power” is defined in 50 U.S.C. § 1801(a) to mean:

- (1) a foreign government or any component thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
- (4) a group engaged in international terrorism or activities in preparation therefor;
- (5) a foreign-based political organization, not substantially composed of United States persons; or
- (6) an entity that is directed and controlled by a foreign government or governments.

⁶ Amending FISA: Hearings before the Senate Select Committee on Intelligence, July 31, 2002 (hereinafter “FISA Hearing”), *available at* [<http://intelligence.senate.gov/0207hr/020731/witness.htm>].

foreign power”⁷ in 50 U.S.C. § 1801(b)(1) (which excludes United States persons⁸). The amendment would add non-U.S. persons⁹ who “engage[] in international terrorism or activities in preparation therefor” to the definition of “agents of a foreign power” for the purposes of FISA. Both the original proposal and the amended language appear to reach the same result: a FISA warrant would be available to investigate a non-U.S. person who engages in international terrorism or activities in preparation therefore without a requirement that there is reason to believe the person is acting on behalf of a terrorist organization, a foreign country, or any entity fitting the definition of “foreign power.” The new definition would sunset with certain other provisions added in P.L. 107-56 on December 31, 2005.¹⁰

The bill’s sponsor says an amendment is necessary to fight foreign terrorists because it is sometimes difficult to show that a proposed target is associated with a foreign power. The new definition would allow the FBI to conduct surveillance on persons who might otherwise evade surveillance through a “loophole” in the present law:

⁷ “Agent of a foreign power” is currently defined in 50 U.S.C. § 1801(b) to mean:

- (1) any person other than a United States person, who —
 - (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
 - (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
- (2) any person who —
 - (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
 - (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
 - (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or
 - (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
 - (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

⁸ “United States person” is defined in 50 U.S.C. § 1801(i) to mean:

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

⁹ “Person” is defined in 50 U.S.C. § 1801(m) to mean:

any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

¹⁰ P.L. 107-56 § 224.

the terrorist who is either acting on his own or the terrorist who, while acting on behalf of an international terrorist organization or state, has not yet clearly signalled that to our law enforcement officials to the point that we can succeed in getting a FISA warrant.¹¹

The case of Zacarias Moussaoui is advanced as a case in point. Although he is a foreign person who was engaged in suspicious activity, the FBI did not approve a request to seek a FISA application to search his computer hard drive because it could not connect him with a foreign government or specific foreign terrorist organization.¹² Some argue that the FBI's misinterpretation of the requirements of FISA, rather than defects in the statute itself led to the failure of the FBI to seek a FISA warrant.¹³ Under this view, the FBI had sufficient information about Moussaoui's connections with Chechen rebels to acquire a FISA warrant, but deciding officials construed FISA to require proof of an association with Al Qaeda or another organization officially listed as a terrorist organization by the State Department.¹⁴ Others interpret the statute to require no certification that the proposed target is associated with any specific group, inasmuch as a "group" of terrorists covered by current law might be as small as two or three persons.¹⁵

The Justice Department supported S. 2586, asserting that the amendment would enable the FBI to target the new type of terrorist threat faced by the United States today. An FBI official describes the new threat, that of the "international Jihad movement" thus:

Historically, terrorism subjects of FBI investigation have been associated with terrorist organizations. As a result, FBI has usually been able to associate an individual with a terrorist organization pled, for FISA purposes, as a foreign power. To a substantial extent, that remains true today. However, we are increasingly seeing terrorist suspects who appear to operate at a distance from these organizations. In perhaps an oversimplification, but illustrative nevertheless, what we see today are (1) agents of foreign powers in the traditional sense who are associated with some organization or discernible group, (2) individuals who appear to have connections with multiple terrorist organizations but who do not appear to owe allegiance to any one of them, but rather owe allegiance to the international Jihad movement and (3)

¹¹ CONG. REC. S10426 (daily ed. Oct. 15, 2002) (statement of Senator Kyl with respect to S. 2586, 107th Congress).

¹² See *id.* Whether a timely search of Moussaoui's computer data would have revealed information that might have allowed the government to prevent the Sept. 11, 2001 attacks is a matter open to debate. See FISA Hearing, *supra* note 6 (Testimony of Jerry Berman, Executive Director, Center for Democracy and Technology)[hereinafter "Berman Testimony"], available at [<http://www.cdt.org/testimony/020731berman.shtml>].

¹³ See *id.*; Beverley Lumpkin, *The 'Lone Wolf,'* ABC News Online, Aug. 2, 2002, at [<http://abcnews.go.com/sections/us/HallsOfJustice/hallsofjustice133.html>].

¹⁴ See Senators Patrick Leahy, Charles Grassley, and Arlen Specter, *Interim Report: FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures*, at 23 -25, Feb. 2003 [hereinafter "Interim Report"] (concluding that FBI officials misapplied the FISA standards for determining whether there was reason to believe Moussaoui was an agent of a foreign power); *Hill Probers Upgrade Evidence Gathered From Moussaoui*, WASH. POST, June 6, 2002, at A18 (reporting reason given by officials for rejecting Minneapolis FBI agent's request for a FISA warrant to search Moussaoui's computer hard drive).

¹⁵ See H.R.Rep. 95-1283, at pt. 1, 74 and n. 38 (1978).

individuals who appear to be personally oriented toward terrorism but with whom there is no known connection to a foreign power.¹⁶

Accordingly, including individuals engaging in terrorist activities or preparations therefore under the definition of “agent of a foreign power” would allow investigators to use FISA to pursue the “lone wolf” terrorist, without the need to show any association to a foreign terrorist group or other foreign power. To treat a United States person as an agent of a foreign power would continue to require a showing that the person is working for or on behalf of a foreign power.¹⁷ In order to obtain a FISA warrant to conduct searches or surveillance with respect to a non-U.S. person as an “agent of a foreign power” under the proposed language, probable cause to believe that the proposed target is engaged or will engage in an act of international terrorism¹⁸ would be required. Critics argue that in the event such evidence is already available, there would be no reason to treat it as anything other than a criminal matter, for which a Title III warrant would be appropriate.¹⁹ Additionally, some question whether there is any rational purpose for treating foreign “lone wolf” terrorists under a separate legal regime from that which applies to “lone wolf” terrorists who are U.S. citizens or permanent resident aliens.²⁰ The Fourth Amendment has been interpreted to cover non-U.S. persons in the United States who are suspected of involvement in criminal activity. Under this view, there is no constitutional reason for treating U.S. persons and non-U.S. persons differently where there is no suspicion of association with a foreign terrorist organization or other foreign power. Some believe, therefore, that the amendment raises significant constitutional issues.²¹

It has also been argued that to divorce FISA from the purpose of gathering foreign intelligence information about foreign powers and their agents, as those terms are normally understood, is a significant departure from the original purpose of the statute and part of the reason courts have held that searches under FISA do not violate the Fourth

¹⁶ See FISA Hearing, *supra* note 6 (Statement for the Record of Marion E. (Spike) Bowman, Deputy General Counsel, Federal Bureau of Investigation).

¹⁷ 50 U.S.C. § 1801(b)(2)(C).

¹⁸ “International terrorism” is defined by 50 U.S.C. § 1801(c) to mean activities that —

- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
- (2) appear to be intended —
 - (A) to intimidate or coerce a civilian population;
 - (B) to influence the policy of a government by intimidation or coercion; or
 - (C) to affect the conduct of a government by assassination or kidnapping; and
- (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

¹⁹ See Berman Testimony, *supra* note 12.

²⁰ See *id.*

²¹ See *id.*; Letter from Kate Martin, Director, Center for National Security Studies, *Proposed Amendments to Foreign Intelligence Surveillance Act*, July 31, 2002.

Amendment.²² The new proposed added definition for “agent of a foreign power” would also broaden other definitions in the statute that are tied to it. For example, “foreign intelligence information” under 50 U.S.C. § 1801(e) would include “information that relates to ... the ability of the United States to protect against ... actual or potential attack or other grave hostile acts of” an individual non-U.S. person suspected of terrorism but unaffiliated with a foreign power, as defined; and “sabotage or international terrorism” committed by same.

On the other hand, the bill’s proponents argue that the new definition, by requiring probable cause that the target is engaging in or preparing for terrorist activity that transcends international boundaries, already meets a high enough standard of particularity to satisfy Title III and constitutional standards.²³ They believe that the interest that the courts have identified to justify the procedures of FISA are not likely to differ appreciably between a case involving a single terrorist and a case involving a group of two or three terrorists, who may be treated as a “foreign power” under existing law.²⁴ Furthermore, the Justice Department argues that the magnitude of harm presented by international terrorists justifies a different set of parameters for determining whether a search is “reasonable” under the Fourth Amendment, which depends on an analysis of whether the government’s interests outweigh any intrusion into individual privacy interests.²⁵ In light of the efforts of international terrorists to obtain weapons of mass destruction, it is argued, a terrorist whose ties to an identified “group” remain obscure presents a grave danger to the United States that outweigh the minimal privacy interests likely to be impacted by the proposed change.

As amended prior to passage in the Senate, S. 113 would require the Attorney General to submit an annual report, in addition to reports already required under FISA, describing the number of times the new authority is used, according to the types of searches or seizures that are conducted, the number of times information obtained through these uses is approved for use by prosecutors in a criminal trial, and any significant court interpretations of the new language that may follow. An amendment that, rather than defining non-United States persons engaging in international terrorism to *be* agents of a foreign power, would have permitted a *presumption* that such persons are agents of a foreign power, was not agreed to.

²² See Berman Testimony, *supra* note 12. Cf. *United States v. United States District Court*, 407 U.S. 297, 308 (1972) (differentiating a domestic intelligence surveillance from a foreign intelligence case because it “require[d] no judgment on the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without the country”); *In re Sealed Case*, 310 F.3d at 746 (same).

²³ See CONG. REC. S10426-28 (daily ed. Oct. 15, 2002) (statement of Senator Kyl with respect to S. 2586 of the 107th Congress).

²⁴ See *id.* at S10430 (citing letter from Daniel J. Bryant, Assistant Attorney General, Department of Justice, Office of Legislative Affairs to Senators Kyl and Schumer).

²⁵ See *FISA Hearing*, *supra* note 6 (Statement for the Record of Marion E. (Spike) Bowman, Deputy General Counsel, Federal Bureau of Investigation), reprinted at CONG. REC. S10430-32 (daily ed. Oct. 15, 2002).

~~SECRET~~

Rowan, J Patrick

From:

Sent:

To:

Subject:

Monday, August 04, 2003 9:06 AM

Rowan, J Patrick

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

BOWMAN MARION

DATE: 01-03-2006
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 01-03-2031

b2

b6

b7C

b5

Pat/Spike

b6

b7C

b5

-----Original Message-----

From:

Sent: Monday, August 04, 2003 9:04 AM

To:

Cc:

Subject:

(S)

(S)

b2

b6

b7C

b5

b1

b1

b2

b6

b7C

b5

/Spike and Pat Rowan

-----Original Message-----

From:

Sent: Saturday, August 02, 2003 12:17 PM

To:

Cc:

Subject:

(S)

(S)

b2

b6

b7C

b5

b1

(S)

~~SECRET~~

~~SECRET~~

(S)

-----Original Message-----

From: [REDACTED]
Sent: Thursday, July 31, 2003 9:57 AM
To: [REDACTED]
Cc: [REDACTED]

Subject: [REDACTED]

b2

b5

b6

b7C

b1

(S)

(S)

(S)

(S)

(S)

(S)

Investigative Law Unit
Office of the General Counsel

~~secret~~

~~SECRET~~



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 30, 2003

To: File

DATE: 01-03-2006
CLASSIFIED BY 65179dmh/baw 05-cv-0845`
REASON: 1.4 (C)
DECLASSIFY ON: 01-03-2031

From: [REDACTED]

b6
b7C

Re: FISA Pen Registers and the Definition of "Content"

On today's date, I had another installment of an ongoing conversation with Spike Bowman concerning the definition of "content" in the context of pen registers sought pursuant to the authority of the Foreign Intelligence Surveillance Act ("FISA") [REDACTED]

b1

(S)

(S)
In short, in a soon to be prepared memorandum on the issue, I will address the discrepancy between the FISA definition of "content" and the definition of content found in the Electronic Communications Privacy Act. Compare 50 U.S.C. Section 1801(n) with 18 U.S.C. Section 2510(8). That memorandum will conclude that, while anomalous, the current FISA definition of content includes, among other things, the "existence" of the communication and "any information concerning the identity of the parties."

b1
(S) b6
b7C

My purpose in conferring today with Spike was to confirm my understanding that while we have an awkward statutory construct that leads us to rely upon a criminal statutory provision to get to the correct Constitutional result we do not today have any legal or ethical impediments to

b1
b6
b7C

(S)

With regard to resolution of the nagging statutory problem and its practical consequences for, among other things, appropriate dissemination of gathered pen register information, I will be conferring later today with Technology Law Branch attorney [REDACTED] and, thereafter, technical guru [REDACTED] to further educate myself on the issue.

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

b6

b7C

Rowan, J Patrick

From:

Sent:

To:

Subject:

Thursday, August 21, 2003 5:17 PM

Rowan, J Patrick

~~**SECRET*~~

Pen Registers and The OLC

(S)

DATE: 12-15-2005

CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845

REASON: 1.4 (c)

DECLASSIFY ON: 12-15-2030

b1

Pat:

In response to your request. I think we can state it fairly succinctly.

b5

(S)

b1

Finally, linking the word [redacted] is classified. Describing the function of the program without the name, however, is unclassified. Hope this helps. I am out of here to the beach. See you after Labor Day. [redacted]

b6

b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

Rowan, J Patrick

From: Rowan, J Patrick
Sent: b6 Thursday, August 21, 2003 4:05 PM
To: [REDACTED]
Cc: b7C BOWMAN, MARION E.; [REDACTED]
Subject: RE: Fun Facts About Pen Registers

DATE: 12-15-2005
CLASSIFIED BY: 65179/DMH/LE/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-15-2030

[REDACTED] I spoke to [REDACTED] about this briefly. I will call over to OLC about an opinion, but I am hoping that you can assist me by putting together two or three paragraphs that I will use to make the request. It does not need to be polished; I am going to use it to make the call, and if they ask for something in writing, we can polish it. [REDACTED]

[REDACTED]

[REDACTED]

(S)

b1

b5

-----Original Message-----

b6

From: [REDACTED]
Sent: Wednesday, August 20, 2003 3:22 PM
To: [REDACTED]
Cc: Rowan, J Patrick; BOWMAN, MARION E.; [REDACTED]
Subject: Fun Facts About Pen Registers

b7C

b6

b1

b7C

b5

(S) [REDACTED] Following up on yesterday's discussion, I spoke earlier today with [REDACTED] program manager for the [REDACTED] [REDACTED] operated out of the Electronic Communications Analysis Unit. A summary of that discussion is attached. As (S)

[REDACTED]

b6

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b7C

<< File [REDACTED] pen.wpu ->

~~SECRET~~

~~SECRET~~

Rowan, J Patrick

From: [REDACTED]
Sent: Wednesday, August 20, 2003 3:22 PM
To: [REDACTED]
Cc: Rowan, J Patrick; BOWMAN, MARION E.; [REDACTED]
Subject: Fun Facts About Pen Registers

DATE: 12-15-2005
CLASSIFIED BY 65179/DMH/LE/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-15-2030

b6

(S)

b7C

(S)

Following up on yesterday's discussion, I spoke earlier today with [REDACTED] program manager for the [REDACTED] [REDACTED] operated out of the Electronic Communications Analysis Unit. A summary of that discussion is attached. As [REDACTED]

[REDACTED]

[REDACTED]



pen.wpd
(11 KB)

b1

b5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

Rowan, J Patrick

From: [REDACTED]
Sent: Wednesday, September 03, 2003 1:56 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

[REDACTED] OGC.

As noted in our prior e-mail [REDACTED]

[REDACTED] Unless OGC objects, [REDACTED] will begin this project in the near future.

SSA [REDACTED]
[REDACTED] Office of Division Counsel [REDACTED]

~~Privileged and Confidential~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-cv-0845

>>> [REDACTED] 09/03 10:48 AM >>>

Thanks for your response; my info. agrees with yours- [REDACTED]

[REDACTED] and [REDACTED] have these substantive matters; [REDACTED]

Let me know what you need from me--SA [REDACTED] researched this problem in February or so, and we recommended that [REDACTED]

Thank you,

[REDACTED] 09/02 6:45 PM >>>
[REDACTED] There is no reason not to since FISA info is readily avail in ACS.

Any word about the FISA-derived information yet?

Thanks,

[REDACTED] b6

b7C

>> [redacted] 08/29 2:33 PM >>>

Many offices do [redacted] OGC has previously taken the position that [redacted]

>>> [redacted] 08/29 2:18 PM >>>

TO: [redacted] Rowan [redacted] OGC

OGC

RE: [redacted]

[redacted] requests that OGC provide guidance regarding [redacted]

[redacted] requests that OGC review and comment on this issue.

SSA [redacted]

Office of Division Counsel [redacted]

Privileged and ~~Confidential~~

>>> [redacted] 08/22 8:36 AM >>>

[redacted] Analyst [redacted] worked with the
TO people and determined it is possible to do, it just isn't done.

Questions:

Please respond when you have a chance.
Thank you,

b6

b7C

b2

b7E

b5

Rowan, J Patrick

From: [REDACTED]
Sent: Friday, August 29, 2003 2:18 PM
To: [REDACTED] Rowan, J Patrick; BOWMAN, MARION E. [REDACTED] b6
[REDACTED] b7C
Cc: [REDACTED]
Subject: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

TO: [REDACTED] Rowan, [REDACTED] OGC b6
[REDACTED] ILU, OGC b7C b2
RE: [REDACTED] b5

requests that OGC provide guidance regarding [REDACTED]

requests that OGC review and comment on this issue.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-0845

----- b2
SSA [REDACTED]
[REDACTED] Office of Division Counsel [REDACTED] b2
Privileged and Confidential b6 b7E
b7C b6 b5
[REDACTED] 08/22 8:36 AM >>>

[REDACTED] Analyst [REDACTED] worked with the
TO people and determined it is possible to do. it just isn't done. [REDACTED]

Questions:

Please respond when you have a chance.
Thank you,
[REDACTED]

b2
b7E
b6
b7C
b5

b6

b7C

Rowan, J Patrick

From: [REDACTED]
Sent: Wednesday, September 03, 2003 2:43 PM
To: [REDACTED]
Cc: [REDACTED] Rowan, J Patrick;
Subject: RE: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

b6

[REDACTED] - I spoke with [REDACTED] and OGC poses no objection to loading FISA [REDACTED] b7C
[REDACTED] as long as the information is flagged as FISA derived. [REDACTED] b2

-----Original Message-----

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-cv-0845

b7E

From: [REDACTED]
Sent: Wednesday, September 03, 2003 1:56 PM
To: [REDACTED]
Cc: [REDACTED]
Rowan, J Patrick; [REDACTED]
Subject: Re: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

b6

b7C

b6

[REDACTED] OGC. b7C

As noted in our prior e-mail - [REDACTED]
[REDACTED]
[REDACTED] Unless OGC objects, [REDACTED] will begin this project in the near
future. b2

b2

b2

b7E

b7E

cc: [REDACTED]
[REDACTED] Office of Division Counsel [REDACTED] b2 b5 b6
Privileged and Confidential b6 b7C

[REDACTED] 09/03 10:48 AM >>> b7C b5

Thanks for your response; my info. agrees with yours. [REDACTED]
[REDACTED]

[REDACTED] and [REDACTED] have these substantive matters. [REDACTED] b2
[REDACTED] b7E
[REDACTED] b6
[REDACTED] b7C

[REDACTED] b5
[REDACTED] b2

Let me know what you need from me--SA [REDACTED] researched this problem in February or so,
and we recommended that [REDACTED] b2
[REDACTED] b7E

Thank you, b6
1 b7C
b5

[redacted]
[redacted]
[redacted] There is no reason not to since FISA info is readily avail in ACS.

b2

[redacted] 09/02 6:45 PM >>>

b7E

Any word about the FISA-derived information yet?

b6

Thanks,

b6

b7C

b7C

b5

>>> [redacted] 08/29 2:33 PM >>>

Many offices do [redacted] OGC has previously taken the position that [redacted]

>>> [redacted] 08/29 2:18 PM >>>

b2

TO: [redacted] Rowan, [redacted] OGC

b6

[redacted] OGC

b7C

b7E

RE: [redacted]

b6

[redacted] requests that OGC provide guidance regarding [redacted]

b7C

b5

[redacted] requests that OGC review and comment on this issue.

b2

b7E

SS: [redacted]
[redacted] Office of Division Counsel [redacted]

b5

~~Privileged and Confidential~~

b6

[redacted] 08/22 8:36 AM >>>

b7C

[redacted]
[redacted] . Analyst [redacted] worked with the
TO people and determined it is possible to do, it just isn't done. [redacted]

b2

b7E

Questions:

b6

b7C

b5

Please respond when you have a chance.

Thank you,

b2

b7E

b6

b7C

b5

TOOLS USED ON THE INTELLIGENCE SIDE

A. FISAs: For searches & surveillance

1. Legal Standard: Probable cause to believe that:
 - (1) the target is a foreign power or an agent of a foreign power
 - (2) that facilities/places at which surveillance is directed is being used, or about to be used, by a foreign power or agent of foreign power
2. "Agent of a foreign power" includes a person who engages in sabotage or international terrorism, or acts in preparation, for or on behalf of a foreign power
3. "Foreign Power" includes a group engaged in international terrorism

B. National Security Letters (NSLs)

1. Analog to criminal subpoenas
2. Used to obtain:
 - a. Telephone and electronic communications records from telephone companies & ISPs
 - b. Records from financial institutions
 - c. Information from credit bureaus
3. USA-Patriot Act expanded our ability to use
 - Eliminated requirement to show by specific & articulate facts that target was "agent of foreign power"
 - Now only requires relevance to a national security investigation
 - Lowered approval levels to SACs (used to be HQ or ADIC)

C. FISA Pen Registers/Trap & Trace Orders

1. New Act also made these easier
 - Again eliminated "agent of foreign power" test
 - Relevance only

USA-Patriot Act: "Uniting & Strengthening America By
Providing Appropriate Tools Required to Intercept & Obstruct Terrorism"

D. FISA Business Records Orders

1. Used to cover only 4 categories (common carriers, public accommodations, vehicle rentals, storage facilities)
2. Now covers all business records
3. Also changed standard to simple relevance

- e) The name, title and address of the communication service provider who should receive the request.
- B. (U) Telephone subscriber and toll records acquired by the foregoing means may be disseminated to other agencies of the Federal Government only when such information is clearly relevant to their authorized responsibilities. *See: id. Section 2709(d).*
- C. (U) On a semiannual basis, the FBI must fully inform the House Permanent Select Committee on Intelligence; the House Committee on the Judiciary; the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary; of requests made by the foregoing means. *See: id. Section 2709(e).*

Section 3-04 (U) Pen Registers and Trap and Trace Devices

- A. (U) Generally, applications for pen registers and trap and trace devices must be submitted to the FISA Court, or to specially designated Federal Magistrates. All such applications must include:
 - 1. The identity of the Federal officer making the application;
 - 2. A certification that the information likely to be obtained is foreign intelligence information not concerning an a USPER; or is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution;
 - 3. Information which demonstrates a reason to believe that the target telephone line, communication instrument or device has been, or is about to be used in communication with: an individual who has or is engaging in international terrorism or clandestine intelligence activities which violate U.S. criminal law; or a foreign power or agent thereof which is engaged in international terrorism or clandestine intelligence activities which violate U.S. criminal law.
- B. (U) Court Orders approving pen registers and trap and trace devices, authorize their installation and operation for periods not to exceed 90 days. Extensions of additional 90 day periods may be obtained.
- C. (U) Notwithstanding the foregoing, however, whenever the Attorney General determines that an emergency exists, and that factual bases exist for a Court Order, the Attorney General may authorize the execution of an emergency pen register or trap and trace device; if the Court is informed at the time of the authorization, and application is in fact made no more than 48 hours after the authorization.
 - 1. Authorized emergency pen registers and trap and trace devices shall terminate when the information sought is obtained, when the application is denied, or 48 hours after the authorization is given, whichever comes first.
 - 2. If a Court Order is denied after an emergency pen register or trap and trace device has been installed, no information collected as a result shall be used in any manner, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.
- D. (U) Notwithstanding the foregoing, the President, acting through the Attorney General, may also authorize the use of a pen register or trap and trace device, without a Court Order, for a

period not to exceed 15 calendar days, following a declaration of war by Congress. See:
Title 50, U.S. Code, Sections 1842-1844.

Section 3-05 (U) Unconsented Electronic Surveillances

- A. (U) The following requirements pertain to the acquisition, retention and dissemination of nonpublic available communications and other information resulting from NFIP ELSURs on foreign powers, and USPER and non-USPER Agents of foreign powers.
- B. (U) Generally, applications for NFIP ELSURs must be submitted to the FISA Court. All such applications must include:
 - 1. The identity of the Federal officer making the application;
 - 2. The approval of the Attorney General, and the President's authority for that approval;
 - 3. The identity or description of the target of the surveillance;
 - 4. A statement of the facts which have led to the belief that: (i) the target is a foreign power or an agent of a foreign power, and that (ii) each of the facilities or places at which the surveillance will be directed is being used, or is about to be used by a foreign power or an agent of a foreign power;
 - 5. A statement of proposed minimization procedures (*see: In the Matter of the Application of the U.S. for an Order Authorizing ELSUR of a Foreign Power, In the Matter of the Application of the U.S. for an Order Authorizing ELSUR of an USPER Agent of a Foreign Power and In the Matter of the Application of the U.S. for an Order Authorizing ELSUR of a Non-USPER Agent of a Foreign Power*);
 - 6. A statement of the nature of the foreign intelligence sought, and the types of communications or activities to be surveilled;
 - 7. A certification by the Assistant to the President for National Security Affairs (or some other presidentially-designated Executive Branch official) that: (i) the certifying official believes the information sought to be foreign intelligence information, (ii) the purpose of the surveillance is to obtain foreign intelligence information, (iii) such information cannot reasonably be obtained by normal investigative techniques; (iv) designates the information sought per set categories and (v) includes a statement explaining the basis for the certification;
 - 8. A statement of the means by which the surveillance will be effected and whether physical entry is required;
 - 9. A statement of the facts concerning all previous applications that have been made involving any of the persons, facilities, or places specified in the application and the actions taken on each previous application;
 - 10. A statement of the period of time for which the surveillance is required and (if the nature of the intelligence gathering is such that approval should not automatically terminate when the described type of information has first been obtained) a description of the facts supporting the belief that additional information of the same type will be obtained thereafter; and
 - 11. Should more than one electronic, mechanical or other device be used with respect to a particular surveillance, a statement regarding the coverage of the devices involved and

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 153

Page 104 ~ Referral/Direct

Page 105 ~ Referral/Direct

Page 106 ~ Referral/Direct

Page 107 ~ Referral/Direct

Page 108 ~ Referral/Direct

Page 109 ~ Referral/Direct

Page 110 ~ Referral/Direct

Page 111 ~ Referral/Direct

Page 112 ~ Referral/Direct

Page 113 ~ Referral/Direct

Page 114 ~ Referral/Direct

Page 115 ~ Referral/Direct

Page 116 ~ Referral/Direct

Page 117 ~ Referral/Direct

Page 118 ~ Referral/Direct

Page 119 ~ Referral/Direct

Page 120 ~ Referral/Direct

Page 121 ~ Referral/Direct

Page 122 ~ Referral/Direct

Page 123 ~ Referral/Direct

Page 124 ~ Referral/Direct

Page 125 ~ Referral/Direct

Page 126 ~ Referral/Direct

Page 127 ~ Referral/Direct

Page 128 ~ Referral/Direct

Page 129 ~ Referral/Direct

Page 130 ~ Referral/Direct

Page 131 ~ Referral/Direct

Page 132 ~ Referral/Direct

Page 133 ~ Referral/Direct

Page 134 ~ Referral/Direct

Page 135 ~ Referral/Direct

Page 136 ~ Referral/Direct

Page 137 ~ Referral/Direct

Page 138 ~ Referral/Direct

Page 139 ~ Referral/Direct

Page 140 ~ Referral/Direct

Page 141 ~ Referral/Direct

Page 142 ~ Referral/Direct

Page 143 ~ Referral/Direct

Page 144 ~ Referral/Direct

Page 192 ~ Referral/Direct

Page 193 ~ Referral/Direct

Page 207 ~ Referral/Direct

Page 208 ~ Referral/Direct
Page 317 ~ Referral/Direct
Page 318 ~ Referral/Direct
Page 319 ~ Referral/Direct
Page 320 ~ Referral/Direct
Page 394 ~ Referral/Direct
Page 395 ~ Referral/Direct
Page 396 ~ Referral/Direct
Page 397 ~ Referral/Direct
Page 398 ~ Referral/Direct
Page 399 ~ Referral/Direct
Page 400 ~ Referral/Direct
Page 401 ~ Referral/Direct
Page 402 ~ Referral/Direct
Page 403 ~ Referral/Direct
Page 404 ~ Referral/Direct
Page 405 ~ Referral/Direct
Page 406 ~ Referral/Direct
Page 407 ~ Referral/Direct
Page 408 ~ Referral/Direct
Page 409 ~ Referral/Direct
Page 410 ~ Referral/Direct
Page 411 ~ Referral/Direct
Page 412 ~ Referral/Direct
Page 413 ~ Referral/Direct
Page 414 ~ Referral/Direct
Page 415 ~ Referral/Direct
Page 416 ~ Referral/Direct
Page 417 ~ Referral/Direct
Page 418 ~ Referral/Direct
Page 419 ~ Referral/Direct
Page 420 ~ Referral/Direct
Page 421 ~ Referral/Direct
Page 422 ~ Referral/Direct
Page 423 ~ Referral/Direct
Page 424 ~ Referral/Direct
Page 425 ~ Referral/Direct
Page 426 ~ Referral/Direct
Page 427 ~ Referral/Direct
Page 428 ~ Referral/Direct
Page 429 ~ Referral/Direct
Page 430 ~ Referral/Direct
Page 431 ~ Referral/Direct
Page 432 ~ Referral/Direct
Page 433 ~ Referral/Direct
Page 434 ~ Referral/Direct
Page 435 ~ Referral/Direct
Page 436 ~ Referral/Direct
Page 437 ~ Referral/Direct
Page 438 ~ Referral/Direct
Page 439 ~ Referral/Direct

Page 440 ~ Referral/Direct
Page 441 ~ Referral/Direct
Page 442 ~ Referral/Direct
Page 443 ~ Referral/Direct
Page 444 ~ Referral/Direct
Page 445 ~ Referral/Direct
Page 446 ~ Referral/Direct
Page 447 ~ Referral/Direct
Page 448 ~ Referral/Direct
Page 449 ~ Referral/Direct
Page 450 ~ Referral/Direct
Page 451 ~ Referral/Direct
Page 452 ~ Referral/Direct
Page 453 ~ Referral/Direct
Page 454 ~ Referral/Direct
Page 455 ~ Referral/Direct
Page 456 ~ Referral/Direct
Page 457 ~ Referral/Direct
Page 458 ~ Referral/Direct
Page 459 ~ Referral/Direct
Page 460 ~ Referral/Direct
Page 461 ~ Referral/Direct
Page 462 ~ Referral/Direct
Page 1020 ~ Duplicate
Page 1021 ~ Referral/Direct
Page 1022 ~ Referral/Direct
Page 1023 ~ Referral/Direct
Page 1024 ~ Referral/Direct
Page 1025 ~ Referral/Direct
Page 1026 ~ Referral/Direct
Page 1027 ~ Referral/Direct
Page 1028 ~ Referral/Direct
Page 1029 ~ Referral/Direct
Page 1030 ~ Referral/Direct
Page 1031 ~ Referral/Direct
Page 1032 ~ Referral/Direct
Page 1033 ~ Referral/Direct
Page 1034 ~ Referral/Direct
Page 1035 ~ Referral/Direct
Page 1036 ~ Referral/Direct
Page 1037 ~ Referral/Direct
Page 1038 ~ Referral/Direct
Page 1039 ~ Referral/Direct
Page 1040 ~ Referral/Direct
Page 1041 ~ Referral/Direct
Page 1042 ~ Referral/Direct
Page 1043 ~ Referral/Direct
Page 1044 ~ Referral/Direct
Page 1045 ~ Referral/Direct
Page 1072 ~ b1, b5, b6, b7C
Page 1073 ~ b1, b5, b6, b7C

Page 1074 ~ b1, b5, b6, b7C
Page 1075 ~ b1, b5, b6, b7C
Page 1076 ~ b1, b5, b6, b7C
Page 1077 ~ b1, b5, b6, b7C
Page 1078 ~ b1, b5, b6, b7C
Page 1079 ~ b1, b5, b6, b7C
Page 1080 ~ b1, b5, b6, b7C

SECTION-BY-SECTION

Section 1. Short Title

This section provides that this Act may be cited as the "FISA Improvements Act of 2005."

Section 2. Duration of FISA Surveillance of Non-United States Persons

Before passage of the USA PATRIOT Act, FISA orders for electronic surveillance targeted against agents of a foreign power had a maximum duration of 90 days and could be extended in 90-day increments, and orders for a physical search could be issued for no more than 45 days, unless the target was a foreign power (in which case, the order could be issued for one year.) *See* 50 U.S.C. §§ 1805(e) and 1824(d) (2000).

Section 207 of the USA PATRIOT Act allows orders for physical searches to be issued for certain agents of foreign powers, including United States persons, for 90 days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and agents of foreign powers that are not United States persons. This section would extend the maximum duration of orders for electronic surveillance and physical search targeted against all agents of foreign powers who are not United States persons. Specifically, initial orders authorizing searches and electronic surveillance would be for periods of up to 120 days, and renewal orders would extend for periods of up to one year.

The USA PATRIOT Act did not amend the permissible duration of orders for pen register/trap and trace surveillance under FISA. The current duration of initial and renewal orders for installation and use of a pen register or trap and trace device is for a period not to exceed 90 days. This section would extend the maximum duration of both